zaid sqae

Audit Report

## Version 1.0

**lhr |** lhr

# Overview

While our organization currently does not have written Policies & Procedures that describe in detail the tasks that we have committed to undertake to adhere to the zaid sqae Cyber Security Framework (CSF). We are committed to adopting one.

We perform a periodic assessment of our environment with regards to the principals and functions set as part of the zaid sqae CSF. The assessment consists of automated scans in conjunction with a review by an Internal Auditor. This document contains both direct evidence of compliance along with attestations by the Internal Auditor based on a review of materials and supporting documentation. The methodology for the review and supporting documentation can be found in the various worksheets and documents (referenced in the zaid sqae Auditor Checklist). Issues are noted in the Risk Analysis and Risk Treatment Plan.

This document supplements the Risk Analysis and Risk Treatment Plan and offer substantiation and verification of policy compliance.

\* The issue is noted in the Risk Treatment Plan.

# Security Officer

Name of Security Officer:

Sqa Cytex

Contact Information for Security Officer:

test1@broadstonetech.com

# Overall Risk

We have performed a Risk Assessment as part of our routine zaid sqae compliance review. See the attached zaid sqae Risk Analysis and zaid sqae Risk Treatment Plan.

# Assets

## **Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.** (NIST-ID.AM)

**NIST-ID.AM.1** Physical devices and systems within the organization are inventoried

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.AM.2** Software platforms and applications within the organization are inventoried

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.AM.3** Organizational communication and data flows are mapped

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.AM.4** External information systems are catalogued

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.AM.5** Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.AM.6** Cybersecurity roles and responsibilities for the entire workforce and third.party stakeholders (e.g., suppliers, customers, partners) are established

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** API Gateway stage logging should be enabled  
**Description:***API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | beta logging not enabled. | Alarm |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** IAM users should be in at least one group  
**Description:***AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | s3readonly not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | taimur associated with IAM group. | Ok |
| **qa tester** | **AWS** | cytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | jediar associated with IAM group. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | testcytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | farrukh associated with IAM group. | Ok |

**Parent** **Control:** DynamoDB table auto scaling should be enabled  
**Description:***Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game autoscaling not enabled. | Alarm |

**Parent** **Control:** VPC flow logs should be enabled  
**Description:***The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | vpc-db2853bf flow logging disabled. | Alarm |

**Parent** **Control:** AWS Config should be enabled  
**Description:***This control checks whether AWS Config is enabled in the account for the local Region and is recording all resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | us-east-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ca-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-north-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | sa-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** Ensure that only approved extensions are installed  
**Description:***For added security only install organization-approved extensions on VMs.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'PHP version' is the latest, if used to run the web app  
**Description:***Periodically newer versions are released for PHP software either due to security flaws or to include additional functionality. Using the latest PHP version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Python version' is the latest stable version, if used to run the web app  
**Description:***Periodically, newer versions are released for Python software either due to security flaws or to include additional functionality. Using the latest Python version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Java version' is the latest, if used to run the web app  
**Description:***Periodically, newer versions are released for Java software either due to security flaws or to include additional functionality. Using the latest Java version for web apps is recommended in order to take advantage of security fixes, if any, and/or new functionalities of the newer version.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'  
**Description:***Limit guest user permissions.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Network Watcher is 'Enabled'  
**Description:***Enable Network Watcher for Azure subscriptions.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in polandcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japaneast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francesouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in qatarcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandnorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwaywest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in swedencentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus3. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaenorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japanwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricanorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanynorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southeastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiasoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in ukwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreasouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uksouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanywestcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwayeast. | Alarm |

**Parent** **Control:** Ensure Cloud Asset Inventory Is Enabled  
**Description:***GCP Cloud Asset Inventory is services that provides a historical view of GCP resources and IAM policies through a time-series database. The information recorded includes metadata on Google Cloud resources, metadata on policies set on Google Cloud projects or resources, and runtime information gathered within a Google Cloud resource.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | cloudasset.googleapis.com Cloud Asset API is disabled. | Alarm |

## **Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.** (NIST-ID.BE)

**NIST-ID.BE.1** The organization’s role in the supply chain is identified and communicated

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.BE.2** The organization’s place in critical infrastructure and its industry sector is identified and communicated

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.BE.3** Priorities for organizational mission, objectives, and activities are established and communicated

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.BE.4** Dependencies and critical functions for delivery of critical services are established

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.BE.5** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** DynamoDB table auto scaling should be enabled  
**Description:***Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game autoscaling not enabled. | Alarm |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

## **Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.** (NIST-ID.GV)

**NIST-ID.GV.1** Organizational information security policy is established

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.GV.2** Information security roles responsibilities are coordinated and aligned with internal roles and external partners

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.GV.3** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.GV.4** Governance and risk management processes address cybersecurity risks

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals** (NIST-ID.RA)

**NIST-ID.RA.1** Asset vulnerabilities are identified and documented

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.RA.2** Cyber threat intelligence is received from information sharing forums and sources

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.RA.3** Threats, both internal and external, are identified and documented

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.RA.4** Potential business impacts and likelihoods are identified

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.RA.5** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.RA.6** Risk responses are identified and prioritized

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Management Console sign-in without MFA  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm console logins that aren't protected by MFA.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for console sign-in without MFA. | Alarm |

**Parent** **Control:** AWS Config should be enabled  
**Description:***This control checks whether AWS Config is enabled in the account for the local Region and is recording all resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | us-east-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ca-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-north-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | sa-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** AWS Security Hub should be enabled for an AWS Account  
**Description:***AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** Ensure a log metric filter and alarm exist for S3 bucket policy changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to S3 bucket policies. Monitoring these changes might reduce time to detect and correct permissive policies on sensitive S3 buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for S3 bucket policy changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for route table changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Routing tables route network traffic between subnets and to network gateways. Security Hub recommends that you create a metric filter and alarm for changes to route tables. Monitoring these changes helps ensure that all VPC traffic flows through an expected path.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for route table changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Management Console authentication failures  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for failed console authentication attempts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for console authentication failures. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Config configuration changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to AWS Config configuration settings. Monitoring these changes helps ensure sustained visibility of configuration items in the account*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for AWS Config configuration changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)  
**Description:***You can do real-time monitoring of API calls 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 in a VPC. Security Hub recommends that you create a metric filter and alarm for changes to NACLs. Monitoring these changes helps ensure that AWS resources and services aren't unintentionally exposed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for changes to NACLs. | Alarm |

**Parent** **Control:** GuardDuty should be enabled  
**Description:***Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** Ensure a log metric filter and alarm exist for changes to network gateways  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Network gateways are required to send and receive traffic to a destination outside a VPC. Security Hub recommends that you create a metric filter and alarm for changes to network gateways.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for changes to network gateways. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for usage of 'root' account  
**Description:***You can do real-time monitoring of API calls directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms.Security Hub recommends that you create a metric filter and alarm for root login attempts. Monitoring for root account logins provides visibility into the use of a fully privileged account and an opportunity to reduce the use of it.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for usage of "root" account. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for CloudTrail configuration changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to CloudTrail configuration settings. Monitoring these changes helps ensure sustained visibility to activities in the account.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for CloudTrail configuration changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for unauthorized API calls  
**Description:***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 recommended that a metric filter and alarm be established for unauthorized API calls.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for unauthorized API calls. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer managed keys  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for customer managed keys that have changed state to disabled or scheduled deletion. Data encrypted with disabled or deleted keys is no longer accessible.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for disabling/deletion of CMKs. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for IAM policy changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes made to IAM policies. Monitoring these changes helps ensure that authentication and authorization controls remain intact.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for IAM policy changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for security group changes  
**Description:***You can do real-time monitoring of API calls 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 in a VPC. Security Hub recommends that you create a metric filter and alarm for changes to security groups. Monitoring these changes helps ensure that resources and services aren't unintentionally exposed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for security group changes. | Alarm |

**Parent** **Control:** CloudWatch alarm should have an action configured  
**Description:***Checks if CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT\_DATA, or OK state. Optionally checks if any actions match a named ARN. The rule is non compliant if there is no action specified for the alarm or optional parameter.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game-WriteCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |
| **qa tester** | **AWS** | High-Low-Game-ReadCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |

**Parent** **Control:** Ensure a log metric filter and alarm exist for VPC changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. You can have more than one VPC in an account, and you can create a peer connection between two VPCs, enabling network traffic to route between VPCs. Security Hub recommends that you create a metric filter and alarm for changes to VPCs.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for VPC changes. | Alarm |

**Parent** **Control:** Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'  
**Description:***Limit guest user permissions.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

## **Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.** (NIST-ID.RM)

**NIST-ID.RM.1** Risk management processes are established, managed, and agreed to by organizational stakeholders

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.RM.2** Organizational risk tolerance is determined and clearly expressed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.RM.3** The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.** (NIST-ID.SC)

**NIST-ID.SC.1** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.SC.2** Identify, prioritize and assess suppliers and third.party partners of information systems, components and services using a cyber supply chain risk assessment process

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.SC.3** Suppliers and 3rd.party partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.SC.4** Suppliers and 3rd.party partners are routinely assessed to confirm that they are meeting their contractual obligations. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-ID.SC.5** Response and recovery planning and testing are conducted with suppliers and third.party providers

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** AWS Config should be enabled  
**Description:***This control checks whether AWS Config is enabled in the account for the local Region and is recording all resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | us-east-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ca-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-north-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | sa-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** GuardDuty should be enabled  
**Description:***Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** Ensure a log metric filter and alarm exist for S3 bucket policy changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to S3 bucket policies. Monitoring these changes might reduce time to detect and correct permissive policies on sensitive S3 buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for S3 bucket policy changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for CloudTrail configuration changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to CloudTrail configuration settings. Monitoring these changes helps ensure sustained visibility to activities in the account.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for CloudTrail configuration changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Config configuration changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to AWS Config configuration settings. Monitoring these changes helps ensure sustained visibility of configuration items in the account*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for AWS Config configuration changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Management Console authentication failures  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for failed console authentication attempts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for console authentication failures. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Management Console sign-in without MFA  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm console logins that aren't protected by MFA.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for console sign-in without MFA. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer managed keys  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for customer managed keys that have changed state to disabled or scheduled deletion. Data encrypted with disabled or deleted keys is no longer accessible.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for disabling/deletion of CMKs. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for IAM policy changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes made to IAM policies. Monitoring these changes helps ensure that authentication and authorization controls remain intact.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for IAM policy changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)  
**Description:***You can do real-time monitoring of API calls 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 in a VPC. Security Hub recommends that you create a metric filter and alarm for changes to NACLs. Monitoring these changes helps ensure that AWS resources and services aren't unintentionally exposed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for changes to NACLs. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for changes to network gateways  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Network gateways are required to send and receive traffic to a destination outside a VPC. Security Hub recommends that you create a metric filter and alarm for changes to network gateways.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for changes to network gateways. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for usage of 'root' account  
**Description:***You can do real-time monitoring of API calls directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms.Security Hub recommends that you create a metric filter and alarm for root login attempts. Monitoring for root account logins provides visibility into the use of a fully privileged account and an opportunity to reduce the use of it.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for usage of "root" account. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for route table changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Routing tables route network traffic between subnets and to network gateways. Security Hub recommends that you create a metric filter and alarm for changes to route tables. Monitoring these changes helps ensure that all VPC traffic flows through an expected path.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for route table changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for security group changes  
**Description:***You can do real-time monitoring of API calls 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 in a VPC. Security Hub recommends that you create a metric filter and alarm for changes to security groups. Monitoring these changes helps ensure that resources and services aren't unintentionally exposed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for security group changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for unauthorized API calls  
**Description:***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 recommended that a metric filter and alarm be established for unauthorized API calls.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for unauthorized API calls. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for VPC changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. You can have more than one VPC in an account, and you can create a peer connection between two VPCs, enabling network traffic to route between VPCs. Security Hub recommends that you create a metric filter and alarm for changes to VPCs.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for VPC changes. | Alarm |

**Parent** **Control:** AWS Security Hub should be enabled for an AWS Account  
**Description:***AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** Ensure Soft Delete is Enabled for Azure Containers and Blob Storage  
**Description:***The Azure Storage blobs contain data like ePHI or Financial, which can be secret or personal. Data that is erroneously modified or deleted by an application or other storage account user will cause data loss or unavailability. It is recommended that both Azure Containers with attached Blob Storage and standalone containers with Blob Storage be made recoverable by enabling the soft delete configuration. This is to save and recover data when blobs or blob snapshots are deleted.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b blobs soft delete disabled. | Alarm |

## **COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.** (SOC2-CC1.1)

**SOC2-CC1.1.1** Sets the Tone at the Top — The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.

**Guidance:** Please provide a listing of all Senior or Executive Management personnel. Please provide a full listing of all Board of Directors (if applicable).Please provide the meeting minutes or agenda from: Management meeting(s) held during the past (6) months. (Please redact any sensitive meeting data)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.1.2** Establishes Standards of Conduct — The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity’s standards of conduct and understood at all levels of the entity and by out-sourced service providers and business partners.

**Guidance:** Please provide the current Employee Handbook. (must be updated with the last 12 months)Please provide the current formal Code of Conduct. (provide only if not included in the Employee Manual or Handbook)Please provide a (blank) Handbook acknowledgement form. (submit only if not included in the handbook)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.1.3** Evaluates Adherence to Standards of Conduct — Processes are in place to evaluate the performance of individuals and teams against the entity’s expected standards of conduct.

**Guidance:** Please provide a (blank) employee evaluation form.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.1.4** Addresses Deviations in a Timely Manner — Deviations from the entity’s expected standards of conduct are identified and remedied in a timely and consistent manner.

**Guidance:** Please provide disciplinary or sanctions policies and procedures. (submit only if not included in the Employee Handbook)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.1.5** Considers Contractors and Vendor Employees in Demonstrating Its Commitment — Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.

**Guidance:** Please provide a (blank) contractor or vendor employee agreement. (if applicable)Please provide contractor or vendor employee onboarding or new hire procedures. (if applicable)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.** (SOC2-CC1.2)

**SOC2-CC1.2.1** Establishes Oversight Responsibilities — The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.

**Guidance:** Please provide the meeting minutes or agenda from: Board of Directors meeting (s) held during the past (6) months or Annual meeting. (Please redact any sensitive meeting data)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.2.2** Applies Relevant Expertise — The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing pofs of senior management and take commensurate action.

**Guidance:** Please provide evidence that the Board of Directors defines, maintains, and periodically evaluates the skills and expertise needed among its members. (if applicable)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.2.3** Operates Independently — The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.

**Guidance:** Please provide a listing of all members of the board of directors and biographies. [Note: Preferably from a published resource] (if applicable)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.2.4** Supplements Board Expertise — The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.

**Guidance:** Please provide evidence that the Board of Directors supplements its expertise through the use of a subcommittee or consultants. (if applicable)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.** (SOC2-CC1.3)

**SOC2-CC1.3.1** Considers All Structures of the Entity — Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.

**Guidance:** Please provide a current organizational chart. (must be updated with the last 12 months)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.3.2** Establishes Reporting Lines — Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.

**Guidance:** The submitted organizational chart (CC1.3.1) must include revision date or please provide evidence of management review.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.3.3** Defines, Assigns, and Limits Authorities and Responsibilities — Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.

**Guidance:** Please provide a sample of (5) current company job descriptions.Please provide documentation or describe procedures for updating job descriptions.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.3.4** Addresses Specific Requirements When Defining Authorities and Responsibilities —Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.

**Guidance:** Within the job descriptions please indicate any requirements relevant to security, availability, and confidentiality. (If applicable)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.3.5** Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities — Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.

**Guidance:** Please provide the Name, Title, and Job description for the current personnel with the responsibility and accountability for vendor management.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** IAM groups should have at least one user  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | developers associated with IAM user. | Ok |
| **qa tester** | **AWS** | Group\_S3 associated with IAM user. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM user. | Ok |
| **qa tester** | **AWS** | ar\_dev associated with IAM user. | Ok |

**Parent** **Control:** IAM groups, users, and roles should not have any inline policies  
**Description:***Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Role Cognito\_dmoat\_sumerianAuth\_Role has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Role Cognito\_dmoat\_sumerianUnauth\_Role has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Role Cognito\_testPoolAuth\_Role has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Role Cognito\_testPoolUnauth\_Role has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Role lambda\_basic\_execution has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Group Group\_S3 has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Group ar\_dev has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Group developers has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Group prytex has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role AmazonSumerianLexPollyTut-CognitoIdentityExampleRo-1J5DCDZ98OBSA has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role AmazonSumerianPollyTutori-CognitoIdentityExampleRo-WZMROL1NX8H4 has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role Tutorial-CognitoIdentityExampleRole-WSU7BA2FIP7W has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role sumerian\_dev has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role sumerian\_dmoat has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role tutorial2-CognitoIdentityExampleRole-2PDP2Y155A1D has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User cytex has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User cytexaudit has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User farrukh has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User jediar has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User prytex has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User s3readonly has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User taimur has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User testcytex has 0 inline policies. | Ok |

**Parent** **Control:** IAM policy should not have statements with admin access  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing 'Effect': 'Allow' with 'Action': '\*' over 'Resource': '\*'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | AWSLambdaEdgeExecutionRole-adc0e8e5-65d9-40a5-aaff-752d94f98e81 contains 0 statements that allow action "\*" on resource "\*". | Ok |
| **qa tester** | **AWS** | cytexaudit\_sploit contains 0 statements that allow action "\*" on resource "\*". | Ok |

**Parent** **Control:** IAM users should be in at least one group  
**Description:***AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | s3readonly not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | taimur associated with IAM group. | Ok |
| **qa tester** | **AWS** | cytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | jediar associated with IAM group. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | testcytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | farrukh associated with IAM group. | Ok |

**Parent** **Control:** IAM user should not have any inline or attached policies  
**Description:***This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | cytexaudit has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | jediar has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | s3readonly has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | taimur has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | testcytex has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | farrukh has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | prytex has 0 inline and 0 directly attached policies. | Ok |

**Parent** **Control:** IAM user credentials that have not been used in 90 days should be disabled  
**Description:***AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex password not enabled  key 1 created 06-Jan-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | cytexaudit password not enabled  key 1 created 02-Mar-2022 never used  key 2 used 01-Sep-2023. | Alarm |
| **qa tester** | **AWS** | farrukh password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | jediar password used 31-Aug-2023  key 1 created 04-Mar-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | prytex password not enabled  key 1 used 26-Aug-2020  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | s3readonly password not enabled  key 1 used 12-Oct-2020  key 2 used 05-Jul-2023. | Alarm |
| **qa tester** | **AWS** | taimur password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | testcytex password used 29-Nov-2021  key 1 not enabled  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | root\_account password used 10-Jul-2023  key 1 not enabled  key 2 not enabled. | Error |

## **COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.** (SOC2-CC1.4)

**SOC2-CC1.4.1** Publish the point of contact for security reports on your website

**Guidance:** Provide your sec.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.4.2** Evaluates Competence and Addresses Shortcomings — The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address short comings.

**Guidance:** Please provide meeting minutes or agenda from (1) management meeting(s) held during the past (3) months. (Please redact any sensitive meeting data)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.4.3** Attracts, Develops, and Retains Individuals — The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.

**Guidance:** Please provide evidence that orientation and annual Information Security Training was conducted - (Training materials, attendance logs, training curriculum, etc.).

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.4.4** Plans and Prepares for Succession — Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.

**Guidance:** Please provide evidence that senior management and the Board of Directors have developed contingency plans for succession.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.4.5** Considers the Background of Individuals — The entity considers the background of potential and existing personnel, contractors and vendor employees when determining whether to employ and retain the individuals.

**Guidance:** Please provide a (blank) background check authorization form.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.4.6** Considers the Technical Competency of Individuals — The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.

**Guidance:** Please provide the current Hiring Policy and procedures - Include new hire checklist. (if applicable)

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.4.7** Provides Training to Maintain Technical Competencies — The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.

**Guidance:** Please provide evidence that orientation and annual Information Security Training was conducted - (Training materials, attendance logs, training curriculum, etc.).

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.** (SOC2-CC1.5)

**SOC2-CC1.5.1** Enforces Accountability Through Structures, Authorities, and Responsibilities — Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.

**Guidance:** Please provide a (blank) background check authorization form.Please provide (5) department meeting conducted from 02/16/19 through current date.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.5.2** Establishes Performance Measures, Incentives, and Rewards — Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.

**Guidance:** Please provide Employee Manual or Handbook including Code of Conduct.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.5.3** Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance — Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.

**Guidance:** Please describe how management and the BOD align incentives with rewards and promotions. Please provide for department goals and indivdual goals.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.5.4** Considers Excessive Pressures — Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.

**Guidance:** Please describe how management and the BOD evaluate and adjust incentives (department and individual) associated with the achievement of company objectives.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**SOC2-CC1.5.5** Evaluates Performance and Rewards or Disciplines Individuals — Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, a provide rewards or exercise disciplinary action, as appropriate.

**Guidance:** Please describe the process for providing feedback and responsibilities going forward after an personnel evaluation.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Establish and implement procedures to create and maintain retrievable exact copies of ePHI.** (HIPAA-3.1)

**Reference:** 164.308a7iiA

**HIPAA-3.1.1** Have you established and implemented procedures to create and maintain retrievable exact copies of ePHI?

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**HIPAA-3.1.2** What types of backups are done of your servers (look at log, rotation schedule offsite storage, testing backups)?.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Backup plan min frequency and min retention check  
**Description:***Checks if a backup plan has a backup rule that satisfies the required frequency and retention period(35 Days). The rule is non compliant if recovery points are not created at least as often as the specified frequency or expire before the specified period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: e8bb8971-d9be-486c-91aa-79d8acbe99ea  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** DynamoDB table auto scaling should be enabled  
**Description:***Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game autoscaling not enabled. | Alarm |

**Parent** **Control:** DynamoDB tables should be in a backup plan  
**Description:***To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: 31b40971-8afb-440c-85fb-75653a3ffe8f  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** DynamoDB table point-in-time recovery should be enabled  
**Description:***Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game point-in-time recovery not enabled. | Alarm |

**Parent** **Control:** DynamoDB table should be protected by backup plan  
**Description:***Ensure if Amazon DynamoDB tables are protected by a backup plan. The rule is non compliant if the DynamoDB Table is not covered by a backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListProtectedResources  https response error StatusCode: 403  RequestID: 8df0f97d-d531-4e9f-aea4-af348c2be4b6  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListProtectedResources because no identity-based policy allows the backup:ListProtectedResources action (SQLSTATE HV000) | Error |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

**Parent** **Control:** A maximum of 3 owners should be designated for your subscription  
**Description:***It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Ok |

**Parent** **Control:** There should be more than one owner assigned to your subscription  
**Description:***It is recommended to designate more than one subscription owner in order to have administrator access redundancy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Alarm |

**Parent** **Control:** External accounts with owner permissions should be removed from your subscription  
**Description:***External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Deprecated accounts with owner permissions should be removed from your subscription  
**Description:***Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Windows machines should meet requirements for 'Security Options - Accounts'  
**Description:***Windows machines should have the specified Group Policy settings in the category 'Security Options - Accounts' for limiting local account use of blank passwords and guest account status. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Ensure that Cloud SQL database instances are configured with automated backups  
**Description:***It is recommended to have all SQL database instances set to enable automated backups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

## **Implement P that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.** (HIPAA-3.2)

**Reference:** 164.310d1

**HIPAA-3.2.1** Have you implemented P that define how hardware and media may be moved into and out of each facility?

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Maintain a record of the movements of hardware and electronic media and any person responsible therefore.** (HIPAA-3.3)

**Reference:** 164.310d2iii

**HIPAA-3.3.1** Do you have and follow a policy to maintain a record of the movements of hardware and electronic media and the person responsible for its movement?

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Ensure Cloud Asset Inventory Is Enabled  
**Description:***GCP Cloud Asset Inventory is services that provides a historical view of GCP resources and IAM policies through a time-series database. The information recorded includes metadata on Google Cloud resources, metadata on policies set on Google Cloud projects or resources, and runtime information gathered within a Google Cloud resource.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | cloudasset.googleapis.com Cloud Asset API is disabled. | Alarm |

**Parent** **Control:** Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects  
**Description:***For the virtual machines where you manage the operating system in Infrastructure as a Service (IaaS), you are responsible for keeping these operating systems and programs up to date. There are multiple ways to manage updates yourself that would be difficult to fit into one recommendation. Check the CIS Benchmarks for each of your Operating Systems as well for potential solutions there. In this recommendation we will use a feature in Google Cloud via its VM manager API to manage updates called Operating System Patch Management (referred to OS Patch Management from here on out). This may requires installing the OS Config API if it is not already installed. Also if you install custom operating systems, they may not functionally support the local OS config agent required to gather operating system patch information and issue update commands. These update commands are the default Linux and Windows commands to install updates such as yum or apt. This feature allows for a central management to issue those commands. OS Patch management also does not host the updates itself, so your VMs will need to be public or be able to access the internet. This is not the only Patch Management solution available to your organization and you should weigh your needs before committing to using this.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

## **Create a retrievable, exact copy of ePHI, when needed, before movement of equipment** (HIPAA-3.4)

**Reference:** 164.310d2iv

**HIPAA-3.4.1** Do you have and follow a plan to create a retrievable, exact copy of ePHI, when needed, before moving equipment on which it is stored?

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Ensure that Cloud SQL database instances are configured with automated backups  
**Description:***It is recommended to have all SQL database instances set to enable automated backups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

## **Define Objectives** (OFDSS-1.1)

**Guidance:** Information Security objectives and accountability for meeting those objectives are best captured in a formal information security policy. This policy should authorize action, establish objectives, and identify accountability for identifying and mitigating information security risks for your organization.

**OFDSS-1.1.1** Identify the security risks that are material to your business, applications, and environments.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-1.1.2** Define how you mitigate the security risks that are material to your business, application, and environments.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** GuardDuty should be enabled  
**Description:***Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

## **Establish Accountability** (OFDSS-1.2)

**Guidance:** Information Security objectives and accountability for meeting those objectives are best captured in a formal information security policy. This policy should authorize action, establish objectives, and identify accountability for identifying and mitigating information security risks for your organization.

**OFDSS-1.2.1** Identify the team or individual that has overall accountability for identifying and mitigating security risks that are material to your business, applications, and environments.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-1.2.2** Identify the teams or individuals responsible for each of the control domains that mitigate the risks that you have identified. For example, owners of controls in the following control domains: a)Asset Management b)Access Controls c) Change Controls d) Cryptography e) Data Minimization f) Incident Management g) Awareness and Training h) Auditing and Alerting i) Network Security j) Vendor Management

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** AWS Config should be enabled  
**Description:***This control checks whether AWS Config is enabled in the account for the local Region and is recording all resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | us-east-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ca-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-north-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | sa-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** GuardDuty should be enabled  
**Description:***Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** Ensure a log metric filter and alarm exist for IAM policy changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes made to IAM policies. Monitoring these changes helps ensure that authentication and authorization controls remain intact.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for IAM policy changes. | Alarm |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** IAM policy should not have statements with admin access  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing 'Effect': 'Allow' with 'Action': '\*' over 'Resource': '\*'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | AWSLambdaEdgeExecutionRole-adc0e8e5-65d9-40a5-aaff-752d94f98e81 contains 0 statements that allow action "\*" on resource "\*". | Ok |
| **qa tester** | **AWS** | cytexaudit\_sploit contains 0 statements that allow action "\*" on resource "\*". | Ok |

**Parent** **Control:** Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)  
**Description:***You can do real-time monitoring of API calls 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 in a VPC. Security Hub recommends that you create a metric filter and alarm for changes to NACLs. Monitoring these changes helps ensure that AWS resources and services aren't unintentionally exposed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for changes to NACLs. | Alarm |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Management Console authentication failures  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for failed console authentication attempts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for console authentication failures. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for usage of 'root' account  
**Description:***You can do real-time monitoring of API calls directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms.Security Hub recommends that you create a metric filter and alarm for root login attempts. Monitoring for root account logins provides visibility into the use of a fully privileged account and an opportunity to reduce the use of it.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for usage of "root" account. | Alarm |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** IAM root user should not have access keys  
**Description:***Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No root user access keys exist. | Ok |

**Parent** **Control:** API Gateway stage logging should be enabled  
**Description:***API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | beta logging not enabled. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress TCP and UDP access from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a does not allow ingress to TCP or UDP ports from 0.0.0.0/0. | Ok |

**Parent** **Control:** Ensure a log metric filter and alarm exist for security group changes  
**Description:***You can do real-time monitoring of API calls 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 in a VPC. Security Hub recommends that you create a metric filter and alarm for changes to security groups. Monitoring these changes helps ensure that resources and services aren't unintentionally exposed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for security group changes. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress SSH access from 0.0.0.0/0  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for SSH from 0.0.0.0/0. | Ok |

**Parent** **Control:** Lambda functions should be in a VPC  
**Description:***Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test is not in VPC. | Alarm |
| **qa tester** | **AWS** | trap\_doors\_lambda is not in VPC. | Alarm |
| **qa tester** | **AWS** | escapeRoomLambdaFunc is not in VPC. | Alarm |
| **qa tester** | **AWS** | esportsgps is not in VPC. | Alarm |
| **qa tester** | **AWS** | medical\_care is not in VPC. | Alarm |

**Parent** **Control:** VPC flow logs should be enabled  
**Description:***The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | vpc-db2853bf flow logging disabled. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for VPC changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. You can have more than one VPC in an account, and you can create a peer connection between two VPCs, enabling network traffic to route between VPCs. Security Hub recommends that you create a metric filter and alarm for changes to VPCs.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for VPC changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer managed keys  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for customer managed keys that have changed state to disabled or scheduled deletion. Data encrypted with disabled or deleted keys is no longer accessible.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for disabling/deletion of CMKs. | Alarm |

**Parent** **Control:** IAM users should be in at least one group  
**Description:***AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | s3readonly not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | taimur associated with IAM group. | Ok |
| **qa tester** | **AWS** | cytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | jediar associated with IAM group. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | testcytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | farrukh associated with IAM group. | Ok |

**Parent** **Control:** IAM user should not have any inline or attached policies  
**Description:***This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | cytexaudit has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | jediar has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | s3readonly has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | taimur has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | testcytex has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | farrukh has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | prytex has 0 inline and 0 directly attached policies. | Ok |

**Parent** **Control:** Ensure a log metric filter and alarm exist for unauthorized API calls  
**Description:***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 recommended that a metric filter and alarm be established for unauthorized API calls.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for unauthorized API calls. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for S3 bucket policy changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to S3 bucket policies. Monitoring these changes might reduce time to detect and correct permissive policies on sensitive S3 buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for S3 bucket policy changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Management Console sign-in without MFA  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm console logins that aren't protected by MFA.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for console sign-in without MFA. | Alarm |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Config configuration changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to AWS Config configuration settings. Monitoring these changes helps ensure sustained visibility of configuration items in the account*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for AWS Config configuration changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for changes to network gateways  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Network gateways are required to send and receive traffic to a destination outside a VPC. Security Hub recommends that you create a metric filter and alarm for changes to network gateways.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for changes to network gateways. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for route table changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Routing tables route network traffic between subnets and to network gateways. Security Hub recommends that you create a metric filter and alarm for changes to route tables. Monitoring these changes helps ensure that all VPC traffic flows through an expected path.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for route table changes. | Alarm |

**Parent** **Control:** AWS Security Hub should be enabled for an AWS Account  
**Description:***AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** DynamoDB table auto scaling should be enabled  
**Description:***Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game autoscaling not enabled. | Alarm |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress access on ports 20, 21, 22, 3306, 3389, 4333 from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for ports 20  21  22  3306  3389  4333 from 0.0.0.0/0. | Ok |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

**Parent** **Control:** Ensure a log metric filter and alarm exist for CloudTrail configuration changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to CloudTrail configuration settings. Monitoring these changes helps ensure sustained visibility to activities in the account.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for CloudTrail configuration changes. | Alarm |

## **Maintain visibility** (OFDSS-2.1)

**Guidance:** Enterprise-grade network gateways, MDM tools, vulnerability scanners, and cloud service management consoles have the ability to discover and provide continuous visibility into your assets on the fly. Depending on the nature of components that make up your technology stack, it may be necessary to rely on a combination of these tools for maintaining high visibility (e.g. network gateway console for visibility into network endpoints connected to your corporate network, and cloud service management console for visibility into your cloud resources). The tools selected must have a mechanism for defining and maintaining the classification of the asset (e.g. production vs. development, or critical vs. non-critical).

**OFDSS-2.1.1** Establish a defined method of listing and identifying all assets and their criticality and sensitivity to the business.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.1.2** Assign responsibility for usage and security of each asset.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.1.3** Maintain clear documentation of network and data flow architectures.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.1.4** Maintain an inventory third party software and libraries in use.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.1.5** Define what is considered a healthy(and therefore trustable) state for each asset.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Storage accounts should use private link  
**Description:***Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not uses private link. | Alarm |

**Parent** **Control:** Storage accounts should restrict network access using virtual network rules  
**Description:***Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b allows network access. | Alarm |

**Parent** **Control:** Vulnerabilities in security configuration on your machines should be remediated  
**Description:***Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Storage account public access should be disallowed  
**Description:***Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not publicy accessible. | Ok |

**Parent** **Control:** Vulnerabilities in Azure Container Registry images should be remediated  
**Description:***Container image vulnerability assessment scans your registry for security vulnerabilities on each pushed container image and exposes detailed findings for each image (powered by Qualys). Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Storage accounts should restrict network access  
**Description:***Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b allows traffic from all networks. | Alarm |

**Parent** **Control:** External accounts with owner permissions should be removed from your subscription  
**Description:***External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Kubernetes cluster pods and containers should only run with approved user and group IDs  
**Description:***Control the user, primary group, supplemental group and file system group IDs that pods and containers can use to run in a Kubernetes Cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Deprecated accounts should be removed from your subscription  
**Description:***Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Non-internet-facing virtual machines should be protected with network security groups  
**Description:***Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Storage accounts should be migrated to new Azure Resource Manager resources  
**Description:***Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b uses azure resource manager. | Ok |

**Parent** **Control:** External accounts with read permissions should be removed from your subscription  
**Description:***External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** SQL servers on machines should have vulnerability findings resolved  
**Description:***SQL vulnerability assessment scans your database for security vulnerabilities, and exposes any deviations from best practices such as misconfigurations, excessive permissions, and unprotected sensitive data. Resolving the vulnerabilities found can greatly improve your database security posture.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Deprecated accounts with owner permissions should be removed from your subscription  
**Description:***Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Adaptive network hardening recommendations should be applied on internet facing virtual machines  
**Description:***Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Vulnerabilities in container security configurations should be remediate  
**Description:***Audit vulnerabilities in security configuration on machines with Docker installed and display as recommendations in Azure Security Center.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** A maximum of 3 owners should be designated for your subscription  
**Description:***It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Ok |

**Parent** **Control:** Adaptive application controls for defining safe applications should be enabled on your machines  
**Description:***Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Vulnerabilities in security configuration on your virtual machine scale sets should be remediated  
**Description:***Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Allowlist rules in your adaptive application control policy should be updated  
**Description:***Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

## **Prevent Dependency Confusion Attacks** (OFDSS-2.2)

**Guidance:** Enforce the use of a central dependency manager with marked scopes for internal and 3rd party dependencies. All developers should be able to connect to the public registry through this central dependency manager. Direct access to public registries should be blocked on the CI/CD servers and on developer machines when possible. Define a process to publish internal dependencies and mandate a security review on them. Register all internal dependencies in respective public registries with the highest version number possible (e.g. 99999.99). Any time a new dependency is published internally, it should be registered before it is used in production assets.

**OFDSS-2.2.1** Use a centralized dependency / package manager to reduce the risk of dependency confusion attacks.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.2.2** Ensure all internal dependencies are downloaded from internal registries for all production environments, including development and CI environments.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.2.3** Whenever possible, verify the checksum of packages before installing.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Allowlist rules in your adaptive application control policy should be updated  
**Description:***Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Log Analytics agent health issues should be resolved on your machines  
**Description:***Security Center uses the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA). To make sure your virtual machines are successfully monitored, you need to make sure the agent is installed on the virtual machines and properly collects security events to the configured workspace.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Kubernetes cluster pods and containers should only run with approved user and group IDs  
**Description:***Control the user, primary group, supplemental group and file system group IDs that pods and containers can use to run in a Kubernetes Cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Adaptive application controls for defining safe applications should be enabled on your machines  
**Description:***Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Storage accounts should restrict network access  
**Description:***Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b allows traffic from all networks. | Alarm |

**Parent** **Control:** There should be more than one owner assigned to your subscription  
**Description:***It is recommended to designate more than one subscription owner in order to have administrator access redundancy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Alarm |

**Parent** **Control:** A maximum of 3 owners should be designated for your subscription  
**Description:***It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Ok |

**Parent** **Control:** Auto provisioning of the Log Analytics agent should be enabled on your subscription  
**Description:***To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Automatic provisioning of monitoring agent is off. | Alarm |

**Parent** **Control:** Azure Arc enabled Kubernetes clusters should have Azure Defender's extension installed  
**Description:***Azure Defender's extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Network Watcher should be enabled  
**Description:***Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in polandcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japaneast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francesouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in qatarcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandnorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwaywest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in swedencentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus3. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaenorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japanwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricanorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanynorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southeastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiasoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in ukwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreasouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uksouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanywestcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwayeast. | Alarm |

**Parent** **Control:** Storage accounts should use private link  
**Description:***Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not uses private link. | Alarm |

## **Detect vulnerable third-party dependencies** (OFDSS-2.3)

**Guidance:** All business critical assets should have 3rd party dependency scanning (SCA) enabled, preferably integrated within the CI/CD environment, and regularly scanning for and identifying vulnerable dependencies (direct and transitive). Upgrade, remove, or replace any vulnerable libraries based on the vulnerability SLAs defined for your organization. Integrate SCA scanning on developer machines (e.g. in the IDE itself) and ensure that scans are run before code is committed.

**OFDSS-2.3.1** Deploy an SCA (Software Composition Analysis) solution to assist in creating a comprehensive dependency “bill-of-materials” and detecting vulnerable library versions.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.3.2** Ensure that all library modules go through regular SCA scans.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Endpoint protection solution should be installed on virtual machine scale sets  
**Description:***Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** SQL servers on machines should have vulnerability findings resolved  
**Description:***SQL vulnerability assessment scans your database for security vulnerabilities, and exposes any deviations from best practices such as misconfigurations, excessive permissions, and unprotected sensitive data. Resolving the vulnerabilities found can greatly improve your database security posture.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Vulnerabilities in Azure Container Registry images should be remediated  
**Description:***Container image vulnerability assessment scans your registry for security vulnerabilities on each pushed container image and exposes detailed findings for each image (powered by Qualys). Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Azure Arc enabled Kubernetes clusters should have Azure Defender's extension installed  
**Description:***Azure Defender's extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Monitor missing Endpoint Protection in Azure Security Center  
**Description:***Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Network Watcher should be enabled  
**Description:***Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in polandcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japaneast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francesouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in qatarcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandnorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwaywest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in swedencentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus3. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaenorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japanwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricanorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanynorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southeastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiasoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in ukwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreasouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uksouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanywestcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwayeast. | Alarm |

**Parent** **Control:** Vulnerabilities in container security configurations should be remediate  
**Description:***Audit vulnerabilities in security configuration on machines with Docker installed and display as recommendations in Azure Security Center.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Subscriptions should have a contact email address for security issues  
**Description:***To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to receive email notifications from Security Center.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Additional email addresses not configured. | Alarm |

**Parent** **Control:** Email notification to subscription owner for high severity alerts should be enabled  
**Description:***To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Security Center.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | "All users with the following roles" not set to Owner. | Alarm |

**Parent** **Control:** Vulnerabilities in security configuration on your virtual machine scale sets should be remediated  
**Description:***Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Vulnerabilities in security configuration on your machines should be remediated  
**Description:***Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Auto provisioning of the Log Analytics agent should be enabled on your subscription  
**Description:***To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Automatic provisioning of monitoring agent is off. | Alarm |

**Parent** **Control:** Email notification for high severity alerts should be enabled  
**Description:***To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Security Center.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | "Notify about alerts with the following severity" not set to High. | Alarm |

**Parent** **Control:** Log Analytics agent health issues should be resolved on your machines  
**Description:***Security Center uses the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA). To make sure your virtual machines are successfully monitored, you need to make sure the agent is installed on the virtual machines and properly collects security events to the configured workspace.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

## **Detect first-party code vulnerabilities** (OFDSS-2.4)

**Guidance:** Document the process for running SAST, DAST, and IAST scans:   
Identify a static analysis tool which works for your organization’s tech stack.   
Evaluate rules to reduce False positive rates and integrate the SAST tool into the build process (CI/CD).   
Identify and set up a dynamic analysis tool which works for your organization’s tech stack and set periodic scans on public internet facing applications.   
Identify an IAST tool which works for your organization’s tech stack and bundle the IAST sensor with your application for deployment in the testing region, making sure to execute all business flows for the IAST tool to capture exploitable paths.   
For any new code changes, a static analysis tool should scan the delta and report on any vulnerabilities found.   
A periodic static scan should be set up on the complete code base to run an end to end analysis.   
A security reviewer should triage vulnerabilities to identify true positives, exploitability, severity, etc.   
All identified vulnerabilities should be fixed based on the SLA defined by your organization.

**OFDSS-2.4.1** Ensure that all first-party code undergoes regular static analysis (SAST) scanning.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.4.2** Ensure that all production assets undergo regular dynamic analysis (DAST) scanning to identify runtime vulnerabilities.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Kubernetes cluster pods and containers should only run with approved user and group IDs  
**Description:***Control the user, primary group, supplemental group and file system group IDs that pods and containers can use to run in a Kubernetes Cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Allowlist rules in your adaptive application control policy should be updated  
**Description:***Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Adaptive application controls for defining safe applications should be enabled on your machines  
**Description:***Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

## **Patch vulnerabilities** (OFDSS-2.5)

**Guidance:** Performing recurring scans against all discovered production assets using a robust vulnerability scanner is a good way to detect vulnerabilities. A process must be established to review the output of these scans, determine their materiality to your technology stack, and deploy available patches based on that materiality. Note that the default severity ratings rendered by a vulnerability scanner for findings are in absolute terms and not in relation to your technology stack. For example, it might find a critical SQL injection vulnerability in a library you use in a stack that does not use SQL. Although this is a “critical” vulnerability in absolute terms, it’s not a “critical” vulnerability in relation to an application stack that does not have SQL in any of its paths. Therefore, materiality of vulnerabilities must be assessed in the context of the underlying stack, and not in just absolute terms.

**OFDSS-2.5.1** Establish a process for receiving and monitoring vulnerability and patch announcements.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.5.2** Maintain a regular patch schedule for non-critical security patches, and install critical security patches in a timely manner.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-2.5.3** Regularly patch any exploitable library module version with SLA dependent on the severity of the vulnerability.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** DynamoDB table should be protected by backup plan  
**Description:***Ensure if Amazon DynamoDB tables are protected by a backup plan. The rule is non compliant if the DynamoDB Table is not covered by a backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListProtectedResources  https response error StatusCode: 403  RequestID: 8df0f97d-d531-4e9f-aea4-af348c2be4b6  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListProtectedResources because no identity-based policy allows the backup:ListProtectedResources action (SQLSTATE HV000) | Error |

**Parent** **Control:** AWS Config should be enabled  
**Description:***This control checks whether AWS Config is enabled in the account for the local Region and is recording all resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | us-east-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ca-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-north-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | sa-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** DynamoDB tables should be in a backup plan  
**Description:***To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: 31b40971-8afb-440c-85fb-75653a3ffe8f  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** DynamoDB table auto scaling should be enabled  
**Description:***Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game autoscaling not enabled. | Alarm |

**Parent** **Control:** S3 public access should be blocked at account and bucket levels  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | cytex not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | testing177 not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | jediar not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | prytex not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket all public access blocks enabled. | Ok |

**Parent** **Control:** Backup plan min frequency and min retention check  
**Description:***Checks if a backup plan has a backup rule that satisfies the required frequency and retention period(35 Days). The rule is non compliant if recovery points are not created at least as often as the specified frequency or expire before the specified period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: e8bb8971-d9be-486c-91aa-79d8acbe99ea  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

**Parent** **Control:** VPC subnet auto assign public IP should be disabled  
**Description:***Ensure if Amazon Virtual Private Cloud (Amazon VPC) subnets are assigned a public IP address. The control is compliant if Amazon VPC does not have subnets that are assigned a public IP address. The control is non compliant if Amazon VPC has subnets that are assigned a public IP address.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | subnet-0445eb72 auto assign public IP enabled. | Alarm |
| **qa tester** | **AWS** | subnet-53cb586e auto assign public IP enabled. | Alarm |
| **qa tester** | **AWS** | subnet-35da1a6d auto assign public IP enabled. | Alarm |
| **qa tester** | **AWS** | subnet-4d8b7767 auto assign public IP enabled. | Alarm |

**Parent** **Control:** DynamoDB table point-in-time recovery should be enabled  
**Description:***Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game point-in-time recovery not enabled. | Alarm |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** Kubernetes cluster pods and containers should only run with approved user and group IDs  
**Description:***Control the user, primary group, supplemental group and file system group IDs that pods and containers can use to run in a Kubernetes Cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Allowlist rules in your adaptive application control policy should be updated  
**Description:***Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Adaptive application controls for defining safe applications should be enabled on your machines  
**Description:***Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

## **Protect against malicious code** (OFDSS-2.6)

**Guidance:** The most common and an effective way to protect network endpoints (workstations and mutable server instances) against malicious code is to deploy endpoint security agents on all managed network endpoints. Most enterprise-grade endpoint security tools will provide a mix of features such as signature-based protections against viruses and malware, and host intrusion detection and prevention all through the same tool.

**OFDSS-2.6.1** Utilize malicious code prevention tools at interaction points with the public internet (mutable internet facing servers, laptops / workstations, mobile devices, etc.)

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** S3 bucket object lock should be enabled  
**Description:***Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 object lock not enabled. | Alarm |
| **qa tester** | **AWS** | entjedi object lock not enabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object lock not enabled. | Alarm |
| **qa tester** | **AWS** | jediar object lock not enabled. | Alarm |
| **qa tester** | **AWS** | devicedetector object lock not enabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object lock not enabled. | Alarm |
| **qa tester** | **AWS** | prytex object lock not enabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object lock not enabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object lock not enabled. | Alarm |
| **qa tester** | **AWS** | cytex object lock not enabled. | Alarm |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** All S3 buckets should log S3 data events in CloudTrail  
**Description:***The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | devicedetector object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object-level data events logging disabled. | Alarm |

**Parent** **Control:** VPC flow logs should be enabled  
**Description:***The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | vpc-db2853bf flow logging disabled. | Alarm |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** API Gateway stage cache encryption at rest should be enabled  
**Description:***To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | beta API cache and encryption not enabled. | Alarm |

**Parent** **Control:** SNS topics should be encrypted at rest  
**Description:***To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | dynamodb encryption at rest disabled. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress SSH access from 0.0.0.0/0  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for SSH from 0.0.0.0/0. | Ok |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** VPC security groups should be associated with at least one ENI  
**Description:***This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | default not associated to any ENI. | Alarm |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** GuardDuty should be enabled  
**Description:***Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

**Parent** **Control:** S3 bucket default encryption should be enabled  
**Description:***To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | usdztestingbucket default encryption enabled. | Ok |
| **qa tester** | **AWS** | cytex default encryption enabled. | Ok |
| **qa tester** | **AWS** | prytex default encryption enabled. | Ok |
| **qa tester** | **AWS** | edmsnapshots default encryption enabled. | Ok |
| **qa tester** | **AWS** | devicedetector default encryption enabled. | Ok |
| **qa tester** | **AWS** | bstfintech default encryption enabled. | Ok |
| **qa tester** | **AWS** | bstlegal default encryption enabled. | Ok |
| **qa tester** | **AWS** | entjedi default encryption enabled. | Ok |
| **qa tester** | **AWS** | jediar default encryption enabled. | Ok |
| **qa tester** | **AWS** | testing177 default encryption enabled. | Ok |

**Parent** **Control:** S3 buckets should enforce SSL  
**Description:***To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | edmsnapshots bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | testing177 bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | bstfintech bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | bstlegal bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | devicedetector bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | entjedi bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | jediar bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | prytex bucket policy does not enforce HTTPS. | Alarm |

**Parent** **Control:** Log group encryption at rest should be enabled  
**Description:***To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Group*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | /aws/lambda/trap\_doors\_lambda not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/Color\_Picker not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/HoursOfOperation not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/color\_picker not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/color\_picker\_test not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/color\_tester not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/escapeRoomLambdaFunc not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/esportsgps not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/hello\_world\_test not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/high\_low\_game\_func not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/medical\_care not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/shippingAddress not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/stars\_test not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/testColorFunc not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/test\_test not encrypted at rest. | Alarm |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** AWS Security Hub should be enabled for an AWS Account  
**Description:***AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** Auto provisioning of the Log Analytics agent should be enabled on your subscription  
**Description:***To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Automatic provisioning of monitoring agent is off. | Alarm |

**Parent** **Control:** Monitor missing Endpoint Protection in Azure Security Center  
**Description:***Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Network Watcher should be enabled  
**Description:***Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in polandcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japaneast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francesouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in qatarcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandnorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwaywest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in swedencentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus3. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaenorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japanwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricanorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanynorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southeastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiasoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in ukwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreasouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uksouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanywestcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwayeast. | Alarm |

**Parent** **Control:** Log Analytics agent health issues should be resolved on your machines  
**Description:***Security Center uses the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA). To make sure your virtual machines are successfully monitored, you need to make sure the agent is installed on the virtual machines and properly collects security events to the configured workspace.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Azure Arc enabled Kubernetes clusters should have Azure Defender's extension installed  
**Description:***Azure Defender's extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Endpoint protection solution should be installed on virtual machine scale sets  
**Description:***Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

## **Deliberately control access** (OFDSS-3.1)

**Guidance:** Deliberately controlling access requires establishing and enforcing an internal access controls policy that defines the requirements for   
(1) granting access to an asset,   
(2) reviewing access grants to an asset, and   
(3) revoking access to an asset.  
This policy must identify roles and responsibilities for each of these activities, and require that an individual is only able to have the least number of permissions they need to perform their job responsibilities (this is the concept of least-privileged role-based access controls). A cadence for performing reviews of existing access grants must also be established, and SLAs for event-driven access revokes (e.g. when an employee leaves the company or changes roles) must also be defined.

**OFDSS-3.1.1** Limit access grants to minimum necessary for job role.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-3.1.2** Require authorization for access grants to sensitive assets and data.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-3.1.3** Identify and revoke obsolete access(e.g. upon user termination and when access is no longer needed).

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** IAM root user hardware MFA should be enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | MFA enabled for root account  but the MFA associated is a virtual device. | Alarm |

**Parent** **Control:** IAM root user should not have access keys  
**Description:***Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No root user access keys exist. | Ok |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** IAM user access keys should be rotated at least every 90 days  
**Description:***The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit AKIA6LNQDLNY2UXNZV4Z created 08-Mar-2022 (541 days). | Alarm |
| **qa tester** | **AWS** | cytexaudit AKIA6LNQDLNY5RKMW5YO created 02-Mar-2022 (547 days). | Alarm |
| **qa tester** | **AWS** | jediar AKIA6LNQDLNYQFEAZJFV created 04-Mar-2022 (546 days). | Alarm |
| **qa tester** | **AWS** | prytex AKIA6LNQDLNYQVA7ZH3U created 25-Aug-2020 (1102 days). | Alarm |
| **qa tester** | **AWS** | s3readonly AKIA6LNQDLNYWEAOKYJT created 08-Mar-2022 (541 days). | Alarm |
| **qa tester** | **AWS** | s3readonly AKIA6LNQDLNYRYRZ4OFT created 07-Oct-2020 (1059 days). | Alarm |
| **qa tester** | **AWS** | cytex AKIA6LNQDLNY2O4WV57L created 06-Jan-2022 (603 days). | Alarm |
| **qa tester** | **AWS** | farrukh AKIA6LNQDLNYZTDD3WXR created 16-Jun-2021 (807 days). | Alarm |
| **qa tester** | **AWS** | taimur AKIA6LNQDLNYSKL4WSF3 created 16-Jun-2021 (807 days). | Alarm |

**Parent** **Control:** IAM user should not have any inline or attached policies  
**Description:***This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | cytexaudit has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | jediar has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | s3readonly has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | taimur has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | testcytex has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | farrukh has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | prytex has 0 inline and 0 directly attached policies. | Ok |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** IAM root user MFA should be enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | MFA enabled for root account. | Ok |

**Parent** **Control:** Lambda functions should be in a VPC  
**Description:***Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test is not in VPC. | Alarm |
| **qa tester** | **AWS** | trap\_doors\_lambda is not in VPC. | Alarm |
| **qa tester** | **AWS** | escapeRoomLambdaFunc is not in VPC. | Alarm |
| **qa tester** | **AWS** | esportsgps is not in VPC. | Alarm |
| **qa tester** | **AWS** | medical\_care is not in VPC. | Alarm |

**Parent** **Control:** IAM policy should not have statements with admin access  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing 'Effect': 'Allow' with 'Action': '\*' over 'Resource': '\*'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | AWSLambdaEdgeExecutionRole-adc0e8e5-65d9-40a5-aaff-752d94f98e81 contains 0 statements that allow action "\*" on resource "\*". | Ok |
| **qa tester** | **AWS** | cytexaudit\_sploit contains 0 statements that allow action "\*" on resource "\*". | Ok |

**Parent** **Control:** IAM password policies for users should have strong configurations  
**Description:***The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Strong password policies not configured. | Alarm |

**Parent** **Control:** VPC internet gateways should be attached to authorized vpc  
**Description:***Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | igw-f1468595 attached to vpc-db2853b. | Ok |

**Parent** **Control:** IAM users with console access should have MFA enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testcytex password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | jediar password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | taimur password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | root\_account password login enabled and MFA device configured. | Ok |
| **qa tester** | **AWS** | cytex password login disabled. | Ok |
| **qa tester** | **AWS** | cytexaudit password login disabled. | Ok |
| **qa tester** | **AWS** | farrukh password login enabled and MFA device configured. | Ok |
| **qa tester** | **AWS** | prytex password login disabled. | Ok |
| **qa tester** | **AWS** | s3readonly password login disabled. | Ok |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** IAM user MFA should be enabled  
**Description:***Enable this rule to restrict access to resources in the AWS Cloud.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | cytexaudit MFA device not configured. | Alarm |
| **qa tester** | **AWS** | jediar MFA device not configured. | Alarm |
| **qa tester** | **AWS** | prytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | s3readonly MFA device not configured. | Alarm |
| **qa tester** | **AWS** | taimur MFA device not configured. | Alarm |
| **qa tester** | **AWS** | testcytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | root\_account MFA device configured. | Ok |
| **qa tester** | **AWS** | farrukh MFA device configured. | Ok |

**Parent** **Control:** VPC security groups should restrict ingress SSH access from 0.0.0.0/0  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for SSH from 0.0.0.0/0. | Ok |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** IAM user credentials that have not been used in 90 days should be disabled  
**Description:***AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex password not enabled  key 1 created 06-Jan-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | cytexaudit password not enabled  key 1 created 02-Mar-2022 never used  key 2 used 01-Sep-2023. | Alarm |
| **qa tester** | **AWS** | farrukh password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | jediar password used 31-Aug-2023  key 1 created 04-Mar-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | prytex password not enabled  key 1 used 26-Aug-2020  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | s3readonly password not enabled  key 1 used 12-Oct-2020  key 2 used 05-Jul-2023. | Alarm |
| **qa tester** | **AWS** | taimur password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | testcytex password used 29-Nov-2021  key 1 not enabled  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | root\_account password used 10-Jul-2023  key 1 not enabled  key 2 not enabled. | Error |

**Parent** **Control:** VPC default security group should not allow inbound and outbound traffic  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Default security group sg-7344060a has inbound and outbound rules. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress TCP and UDP access from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a does not allow ingress to TCP or UDP ports from 0.0.0.0/0. | Ok |

**Parent** **Control:** IAM groups should have at least one user  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | developers associated with IAM user. | Ok |
| **qa tester** | **AWS** | Group\_S3 associated with IAM user. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM user. | Ok |
| **qa tester** | **AWS** | ar\_dev associated with IAM user. | Ok |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** IAM users should be in at least one group  
**Description:***AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | s3readonly not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | taimur associated with IAM group. | Ok |
| **qa tester** | **AWS** | cytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | jediar associated with IAM group. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | testcytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | farrukh associated with IAM group. | Ok |

**Parent** **Control:** VPC security groups should restrict ingress access on ports 20, 21, 22, 3306, 3389, 4333 from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for ports 20  21  22  3306  3389  4333 from 0.0.0.0/0. | Ok |

**Parent** **Control:** External accounts with read permissions should be removed from your subscription  
**Description:***External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Deprecated accounts with owner permissions should be removed from your subscription  
**Description:***Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Storage accounts should be migrated to new Azure Resource Manager resources  
**Description:***Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b uses azure resource manager. | Ok |

**Parent** **Control:** External accounts with owner permissions should be removed from your subscription  
**Description:***External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Deprecated accounts should be removed from your subscription  
**Description:***Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** There should be more than one owner assigned to your subscription  
**Description:***It is recommended to designate more than one subscription owner in order to have administrator access redundancy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Alarm |

**Parent** **Control:** A maximum of 3 owners should be designated for your subscription  
**Description:***It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Ok |

## **Ensure segregation of duties (SoD)** (OFDSS-3.2)

**Guidance:** Segregation of duties between the grantor (individual performing the access grant), grantee (individual receiving the access), and the approver (individual authorizing the access) must be maintained.

**OFDSS-3.2.1** Prevent individuals from granting access to themselves, reviewing their own access, and approving their own access.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** IAM groups, users, and roles should not have any inline policies  
**Description:***Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Role Cognito\_dmoat\_sumerianAuth\_Role has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Role Cognito\_dmoat\_sumerianUnauth\_Role has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Role Cognito\_testPoolAuth\_Role has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Role Cognito\_testPoolUnauth\_Role has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Role lambda\_basic\_execution has 1 inline policies. | Alarm |
| **qa tester** | **AWS** | Group Group\_S3 has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Group ar\_dev has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Group developers has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Group prytex has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role AmazonSumerianLexPollyTut-CognitoIdentityExampleRo-1J5DCDZ98OBSA has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role AmazonSumerianPollyTutori-CognitoIdentityExampleRo-WZMROL1NX8H4 has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role Tutorial-CognitoIdentityExampleRole-WSU7BA2FIP7W has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role sumerian\_dev has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role sumerian\_dmoat has 0 inline policies. | Ok |
| **qa tester** | **AWS** | Role tutorial2-CognitoIdentityExampleRole-2PDP2Y155A1D has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User cytex has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User cytexaudit has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User farrukh has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User jediar has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User prytex has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User s3readonly has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User taimur has 0 inline policies. | Ok |
| **qa tester** | **AWS** | User testcytex has 0 inline policies. | Ok |

**Parent** **Control:** IAM policy should not have statements with admin access  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing 'Effect': 'Allow' with 'Action': '\*' over 'Resource': '\*'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | AWSLambdaEdgeExecutionRole-adc0e8e5-65d9-40a5-aaff-752d94f98e81 contains 0 statements that allow action "\*" on resource "\*". | Ok |
| **qa tester** | **AWS** | cytexaudit\_sploit contains 0 statements that allow action "\*" on resource "\*". | Ok |

**Parent** **Control:** IAM root user should not have access keys  
**Description:***Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No root user access keys exist. | Ok |

**Parent** **Control:** IAM users should be in at least one group  
**Description:***AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | s3readonly not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | taimur associated with IAM group. | Ok |
| **qa tester** | **AWS** | cytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | jediar associated with IAM group. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | testcytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | farrukh associated with IAM group. | Ok |

**Parent** **Control:** IAM user should not have any inline or attached policies  
**Description:***This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | cytexaudit has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | jediar has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | s3readonly has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | taimur has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | testcytex has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | farrukh has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | prytex has 0 inline and 0 directly attached policies. | Ok |

**Parent** **Control:** IAM user credentials that have not been used in 90 days should be disabled  
**Description:***AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex password not enabled  key 1 created 06-Jan-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | cytexaudit password not enabled  key 1 created 02-Mar-2022 never used  key 2 used 01-Sep-2023. | Alarm |
| **qa tester** | **AWS** | farrukh password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | jediar password used 31-Aug-2023  key 1 created 04-Mar-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | prytex password not enabled  key 1 used 26-Aug-2020  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | s3readonly password not enabled  key 1 used 12-Oct-2020  key 2 used 05-Jul-2023. | Alarm |
| **qa tester** | **AWS** | taimur password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | testcytex password used 29-Nov-2021  key 1 not enabled  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | root\_account password used 10-Jul-2023  key 1 not enabled  key 2 not enabled. | Error |

**Parent** **Control:** Lambda functions should be in a VPC  
**Description:***Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test is not in VPC. | Alarm |
| **qa tester** | **AWS** | trap\_doors\_lambda is not in VPC. | Alarm |
| **qa tester** | **AWS** | escapeRoomLambdaFunc is not in VPC. | Alarm |
| **qa tester** | **AWS** | esportsgps is not in VPC. | Alarm |
| **qa tester** | **AWS** | medical\_care is not in VPC. | Alarm |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** S3 public access should be blocked at bucket levels  
**Description:***Ensure if Amazon Simple Storage Service (Amazon S3) buckets are publicly accessible. This rule is non compliant if an Amazon S3 bucket is not listed in the excludedPublicBuckets parameter and bucket level settings are public.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | cytex not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | jediar not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | prytex not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket all public access blocks enabled. | Ok |

**Parent** **Control:** VPC subnet auto assign public IP should be disabled  
**Description:***Ensure if Amazon Virtual Private Cloud (Amazon VPC) subnets are assigned a public IP address. The control is compliant if Amazon VPC does not have subnets that are assigned a public IP address. The control is non compliant if Amazon VPC has subnets that are assigned a public IP address.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | subnet-0445eb72 auto assign public IP enabled. | Alarm |
| **qa tester** | **AWS** | subnet-53cb586e auto assign public IP enabled. | Alarm |
| **qa tester** | **AWS** | subnet-35da1a6d auto assign public IP enabled. | Alarm |
| **qa tester** | **AWS** | subnet-4d8b7767 auto assign public IP enabled. | Alarm |

**Parent** **Control:** External accounts with read permissions should be removed from your subscription  
**Description:***External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Deprecated accounts with owner permissions should be removed from your subscription  
**Description:***Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Storage accounts should be migrated to new Azure Resource Manager resources  
**Description:***Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b uses azure resource manager. | Ok |

**Parent** **Control:** External accounts with owner permissions should be removed from your subscription  
**Description:***External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Deprecated accounts should be removed from your subscription  
**Description:***Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** There should be more than one owner assigned to your subscription  
**Description:***It is recommended to designate more than one subscription owner in order to have administrator access redundancy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Alarm |

**Parent** **Control:** A maximum of 3 owners should be designated for your subscription  
**Description:***It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Ok |

## **Use strong authentication** (OFDSS-3.3)

**Guidance:** Authentication for all critical assets must be deployed to require something that the user knows (e.g. username and password) and something that the user has in their possession (e.g. a push notification to an authenticator app in the user’s possession). 2FA layers that rely on static responses, such as question-based 2FA, should not be used as they do not rely on something that the user has in their possession, therefore, are considered an ineffective form of 2FA.

**OFDSS-3.3.1** Utilize industry-accepted strong protocols for authenticating users (e.g. something you know and something you have).

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-3.3.2** Escalate strength of authentication based on asset criticality.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** IAM users with console access should have MFA enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testcytex password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | jediar password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | taimur password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | root\_account password login enabled and MFA device configured. | Ok |
| **qa tester** | **AWS** | cytex password login disabled. | Ok |
| **qa tester** | **AWS** | cytexaudit password login disabled. | Ok |
| **qa tester** | **AWS** | farrukh password login enabled and MFA device configured. | Ok |
| **qa tester** | **AWS** | prytex password login disabled. | Ok |
| **qa tester** | **AWS** | s3readonly password login disabled. | Ok |

**Parent** **Control:** VPC security groups should restrict ingress SSH access from 0.0.0.0/0  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for SSH from 0.0.0.0/0. | Ok |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** IAM policy should not have statements with admin access  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing 'Effect': 'Allow' with 'Action': '\*' over 'Resource': '\*'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | AWSLambdaEdgeExecutionRole-adc0e8e5-65d9-40a5-aaff-752d94f98e81 contains 0 statements that allow action "\*" on resource "\*". | Ok |
| **qa tester** | **AWS** | cytexaudit\_sploit contains 0 statements that allow action "\*" on resource "\*". | Ok |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** IAM root user MFA should be enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | MFA enabled for root account. | Ok |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** VPC internet gateways should be attached to authorized vpc  
**Description:***Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | igw-f1468595 attached to vpc-db2853b. | Ok |

**Parent** **Control:** IAM user access keys should be rotated at least every 90 days  
**Description:***The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit AKIA6LNQDLNY2UXNZV4Z created 08-Mar-2022 (541 days). | Alarm |
| **qa tester** | **AWS** | cytexaudit AKIA6LNQDLNY5RKMW5YO created 02-Mar-2022 (547 days). | Alarm |
| **qa tester** | **AWS** | jediar AKIA6LNQDLNYQFEAZJFV created 04-Mar-2022 (546 days). | Alarm |
| **qa tester** | **AWS** | prytex AKIA6LNQDLNYQVA7ZH3U created 25-Aug-2020 (1102 days). | Alarm |
| **qa tester** | **AWS** | s3readonly AKIA6LNQDLNYWEAOKYJT created 08-Mar-2022 (541 days). | Alarm |
| **qa tester** | **AWS** | s3readonly AKIA6LNQDLNYRYRZ4OFT created 07-Oct-2020 (1059 days). | Alarm |
| **qa tester** | **AWS** | cytex AKIA6LNQDLNY2O4WV57L created 06-Jan-2022 (603 days). | Alarm |
| **qa tester** | **AWS** | farrukh AKIA6LNQDLNYZTDD3WXR created 16-Jun-2021 (807 days). | Alarm |
| **qa tester** | **AWS** | taimur AKIA6LNQDLNYSKL4WSF3 created 16-Jun-2021 (807 days). | Alarm |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** IAM password policies for users should have strong configurations  
**Description:***The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Strong password policies not configured. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress access on ports 20, 21, 22, 3306, 3389, 4333 from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for ports 20  21  22  3306  3389  4333 from 0.0.0.0/0. | Ok |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** IAM groups should have at least one user  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | developers associated with IAM user. | Ok |
| **qa tester** | **AWS** | Group\_S3 associated with IAM user. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM user. | Ok |
| **qa tester** | **AWS** | ar\_dev associated with IAM user. | Ok |

**Parent** **Control:** IAM user should not have any inline or attached policies  
**Description:***This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | cytexaudit has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | jediar has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | s3readonly has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | taimur has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | testcytex has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | farrukh has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | prytex has 0 inline and 0 directly attached policies. | Ok |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** IAM user credentials that have not been used in 90 days should be disabled  
**Description:***AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex password not enabled  key 1 created 06-Jan-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | cytexaudit password not enabled  key 1 created 02-Mar-2022 never used  key 2 used 01-Sep-2023. | Alarm |
| **qa tester** | **AWS** | farrukh password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | jediar password used 31-Aug-2023  key 1 created 04-Mar-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | prytex password not enabled  key 1 used 26-Aug-2020  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | s3readonly password not enabled  key 1 used 12-Oct-2020  key 2 used 05-Jul-2023. | Alarm |
| **qa tester** | **AWS** | taimur password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | testcytex password used 29-Nov-2021  key 1 not enabled  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | root\_account password used 10-Jul-2023  key 1 not enabled  key 2 not enabled. | Error |

**Parent** **Control:** VPC security groups should restrict ingress TCP and UDP access from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a does not allow ingress to TCP or UDP ports from 0.0.0.0/0. | Ok |

**Parent** **Control:** VPC default security group should not allow inbound and outbound traffic  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Default security group sg-7344060a has inbound and outbound rules. | Alarm |

**Parent** **Control:** IAM root user hardware MFA should be enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | MFA enabled for root account  but the MFA associated is a virtual device. | Alarm |

**Parent** **Control:** IAM users should be in at least one group  
**Description:***AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | s3readonly not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | taimur associated with IAM group. | Ok |
| **qa tester** | **AWS** | cytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | jediar associated with IAM group. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | testcytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | farrukh associated with IAM group. | Ok |

**Parent** **Control:** IAM user MFA should be enabled  
**Description:***Enable this rule to restrict access to resources in the AWS Cloud.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | cytexaudit MFA device not configured. | Alarm |
| **qa tester** | **AWS** | jediar MFA device not configured. | Alarm |
| **qa tester** | **AWS** | prytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | s3readonly MFA device not configured. | Alarm |
| **qa tester** | **AWS** | taimur MFA device not configured. | Alarm |
| **qa tester** | **AWS** | testcytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | root\_account MFA device configured. | Ok |
| **qa tester** | **AWS** | farrukh MFA device configured. | Ok |

**Parent** **Control:** Lambda functions should be in a VPC  
**Description:***Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test is not in VPC. | Alarm |
| **qa tester** | **AWS** | trap\_doors\_lambda is not in VPC. | Alarm |
| **qa tester** | **AWS** | escapeRoomLambdaFunc is not in VPC. | Alarm |
| **qa tester** | **AWS** | esportsgps is not in VPC. | Alarm |
| **qa tester** | **AWS** | medical\_care is not in VPC. | Alarm |

**Parent** **Control:** IAM root user should not have access keys  
**Description:***Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No root user access keys exist. | Ok |

**Parent** **Control:** Deprecated accounts with owner permissions should be removed from your subscription  
**Description:***Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Storage accounts should be migrated to new Azure Resource Manager resources  
**Description:***Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b uses azure resource manager. | Ok |

**Parent** **Control:** Adaptive network hardening recommendations should be applied on internet facing virtual machines  
**Description:***Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** A maximum of 3 owners should be designated for your subscription  
**Description:***It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | 1 owner(s) associated. | Ok |

**Parent** **Control:** Non-internet-facing virtual machines should be protected with network security groups  
**Description:***Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Deprecated accounts should be removed from your subscription  
**Description:***Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Storage accounts should restrict network access using virtual network rules  
**Description:***Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b allows network access. | Alarm |

**Parent** **Control:** Storage accounts should restrict network access  
**Description:***Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b allows traffic from all networks. | Alarm |

**Parent** **Control:** Storage accounts should use private link  
**Description:***Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not uses private link. | Alarm |

**Parent** **Control:** Storage account public access should be disallowed  
**Description:***Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not publicy accessible. | Ok |

**Parent** **Control:** External accounts with read permissions should be removed from your subscription  
**Description:***External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** External accounts with owner permissions should be removed from your subscription  
**Description:***External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

## **Harden points of authentication** (OFDSS-3.4)

**Guidance:** Authentication behavior of legitimate users tends to be predictable under most circumstances. The number of authentication attempts that a user is allowed should be defined, and requests that breach this threshold should be rate limited at points of authentication.

**OFDSS-3.4.1** Ensure rate-limiting mechanisms are in place at points of authentication.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**OFDSS-3.4.2** Ensure access defaults to DENY, and DENY in case of failure of the authentication mechanisms.

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** VPC security groups should restrict ingress access on ports 20, 21, 22, 3306, 3389, 4333 from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for ports 20  21  22  3306  3389  4333 from 0.0.0.0/0. | Ok |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** IAM user access keys should be rotated at least every 90 days  
**Description:***The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit AKIA6LNQDLNY2UXNZV4Z created 08-Mar-2022 (541 days). | Alarm |
| **qa tester** | **AWS** | cytexaudit AKIA6LNQDLNY5RKMW5YO created 02-Mar-2022 (547 days). | Alarm |
| **qa tester** | **AWS** | jediar AKIA6LNQDLNYQFEAZJFV created 04-Mar-2022 (546 days). | Alarm |
| **qa tester** | **AWS** | prytex AKIA6LNQDLNYQVA7ZH3U created 25-Aug-2020 (1102 days). | Alarm |
| **qa tester** | **AWS** | s3readonly AKIA6LNQDLNYWEAOKYJT created 08-Mar-2022 (541 days). | Alarm |
| **qa tester** | **AWS** | s3readonly AKIA6LNQDLNYRYRZ4OFT created 07-Oct-2020 (1059 days). | Alarm |
| **qa tester** | **AWS** | cytex AKIA6LNQDLNY2O4WV57L created 06-Jan-2022 (603 days). | Alarm |
| **qa tester** | **AWS** | farrukh AKIA6LNQDLNYZTDD3WXR created 16-Jun-2021 (807 days). | Alarm |
| **qa tester** | **AWS** | taimur AKIA6LNQDLNYSKL4WSF3 created 16-Jun-2021 (807 days). | Alarm |

**Parent** **Control:** IAM user MFA should be enabled  
**Description:***Enable this rule to restrict access to resources in the AWS Cloud.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | cytexaudit MFA device not configured. | Alarm |
| **qa tester** | **AWS** | jediar MFA device not configured. | Alarm |
| **qa tester** | **AWS** | prytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | s3readonly MFA device not configured. | Alarm |
| **qa tester** | **AWS** | taimur MFA device not configured. | Alarm |
| **qa tester** | **AWS** | testcytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | root\_account MFA device configured. | Ok |
| **qa tester** | **AWS** | farrukh MFA device configured. | Ok |

**Parent** **Control:** IAM user credentials that have not been used in 90 days should be disabled  
**Description:***AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex password not enabled  key 1 created 06-Jan-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | cytexaudit password not enabled  key 1 created 02-Mar-2022 never used  key 2 used 01-Sep-2023. | Alarm |
| **qa tester** | **AWS** | farrukh password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | jediar password used 31-Aug-2023  key 1 created 04-Mar-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | prytex password not enabled  key 1 used 26-Aug-2020  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | s3readonly password not enabled  key 1 used 12-Oct-2020  key 2 used 05-Jul-2023. | Alarm |
| **qa tester** | **AWS** | taimur password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | testcytex password used 29-Nov-2021  key 1 not enabled  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | root\_account password used 10-Jul-2023  key 1 not enabled  key 2 not enabled. | Error |

**Parent** **Control:** IAM password policies for users should have strong configurations  
**Description:***The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Strong password policies not configured. | Alarm |

**Parent** **Control:** IAM user should not have any inline or attached policies  
**Description:***This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | cytexaudit has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | jediar has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | s3readonly has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | taimur has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | testcytex has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | farrukh has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | prytex has 0 inline and 0 directly attached policies. | Ok |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress TCP and UDP access from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a does not allow ingress to TCP or UDP ports from 0.0.0.0/0. | Ok |

**Parent** **Control:** IAM policy should not have statements with admin access  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing 'Effect': 'Allow' with 'Action': '\*' over 'Resource': '\*'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | AWSLambdaEdgeExecutionRole-adc0e8e5-65d9-40a5-aaff-752d94f98e81 contains 0 statements that allow action "\*" on resource "\*". | Ok |
| **qa tester** | **AWS** | cytexaudit\_sploit contains 0 statements that allow action "\*" on resource "\*". | Ok |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** IAM users should be in at least one group  
**Description:***AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | s3readonly not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | taimur associated with IAM group. | Ok |
| **qa tester** | **AWS** | cytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | jediar associated with IAM group. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | testcytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | farrukh associated with IAM group. | Ok |

**Parent** **Control:** IAM root user hardware MFA should be enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | MFA enabled for root account  but the MFA associated is a virtual device. | Alarm |

**Parent** **Control:** IAM root user MFA should be enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | MFA enabled for root account. | Ok |

**Parent** **Control:** VPC internet gateways should be attached to authorized vpc  
**Description:***Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | igw-f1468595 attached to vpc-db2853b. | Ok |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress SSH access from 0.0.0.0/0  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for SSH from 0.0.0.0/0. | Ok |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** IAM groups should have at least one user  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | developers associated with IAM user. | Ok |
| **qa tester** | **AWS** | Group\_S3 associated with IAM user. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM user. | Ok |
| **qa tester** | **AWS** | ar\_dev associated with IAM user. | Ok |

**Parent** **Control:** Lambda functions should be in a VPC  
**Description:***Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test is not in VPC. | Alarm |
| **qa tester** | **AWS** | trap\_doors\_lambda is not in VPC. | Alarm |
| **qa tester** | **AWS** | escapeRoomLambdaFunc is not in VPC. | Alarm |
| **qa tester** | **AWS** | esportsgps is not in VPC. | Alarm |
| **qa tester** | **AWS** | medical\_care is not in VPC. | Alarm |

**Parent** **Control:** IAM users with console access should have MFA enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testcytex password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | jediar password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | taimur password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | root\_account password login enabled and MFA device configured. | Ok |
| **qa tester** | **AWS** | cytex password login disabled. | Ok |
| **qa tester** | **AWS** | cytexaudit password login disabled. | Ok |
| **qa tester** | **AWS** | farrukh password login enabled and MFA device configured. | Ok |
| **qa tester** | **AWS** | prytex password login disabled. | Ok |
| **qa tester** | **AWS** | s3readonly password login disabled. | Ok |

**Parent** **Control:** VPC default security group should not allow inbound and outbound traffic  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Default security group sg-7344060a has inbound and outbound rules. | Alarm |

**Parent** **Control:** IAM root user should not have access keys  
**Description:***Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No root user access keys exist. | Ok |

**Parent** **Control:** Vulnerabilities in security configuration on your virtual machine scale sets should be remediated  
**Description:***Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Endpoint protection solution should be installed on virtual machine scale sets  
**Description:***Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Storage accounts should have infrastructure encryption  
**Description:***Enable infrastructure encryption for higher level of assurance that the data is secure. When infrastructure encryption is enabled, data in a storage account is encrypted twice.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b infrastructure encryption disabled. | Alarm |

**Parent** **Control:** Non-internet-facing virtual machines should be protected with network security groups  
**Description:***Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Network Watcher should be enabled  
**Description:***Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in polandcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japaneast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francesouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in qatarcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandnorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwaywest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in swedencentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus3. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaenorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japanwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricanorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanynorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southeastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiasoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in ukwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreasouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uksouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanywestcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwayeast. | Alarm |

**Parent** **Control:** Vulnerabilities in security configuration on your machines should be remediated  
**Description:***Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Azure Arc enabled Kubernetes clusters should have Azure Defender's extension installed  
**Description:***Azure Defender's extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Subscriptions should have a contact email address for security issues  
**Description:***To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to receive email notifications from Security Center.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Additional email addresses not configured. | Alarm |

**Parent** **Control:** Email notification to subscription owner for high severity alerts should be enabled  
**Description:***To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Security Center.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | "All users with the following roles" not set to Owner. | Alarm |

**Parent** **Control:** Adaptive network hardening recommendations should be applied on internet facing virtual machines  
**Description:***Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources  
**Description:***Virtual machines without an enabled disk encryption will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Secure transfer to storage accounts should be enabled  
**Description:***Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b encryption in transit enabled. | Ok |

**Parent** **Control:** Storage account public access should be disallowed  
**Description:***Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not publicy accessible. | Ok |

**Parent** **Control:** Storage accounts should restrict network access  
**Description:***Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b allows traffic from all networks. | Alarm |

**Parent** **Control:** Auto provisioning of the Log Analytics agent should be enabled on your subscription  
**Description:***To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Automatic provisioning of monitoring agent is off. | Alarm |

**Parent** **Control:** Email notification for high severity alerts should be enabled  
**Description:***To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Security Center.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | "Notify about alerts with the following severity" not set to High. | Alarm |

**Parent** **Control:** Storage accounts should use private link  
**Description:***Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not uses private link. | Alarm |

**Parent** **Control:** Log Analytics agent health issues should be resolved on your machines  
**Description:***Security Center uses the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA). To make sure your virtual machines are successfully monitored, you need to make sure the agent is installed on the virtual machines and properly collects security events to the configured workspace.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Monitor missing Endpoint Protection in Azure Security Center  
**Description:***Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Storage accounts should restrict network access using virtual network rules  
**Description:***Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b allows network access. | Alarm |

**Parent** **Control:** Storage accounts should use customer-managed key for encryption  
**Description:***Secure your storage account with greater flexibility using customer-managed keys. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Using customer-managed keys provides additional capabilities to control rotation of the key encryption key or cryptographically erase data.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not encrypted with CMK. | Alarm |

## **Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.** (PCI DSS V4-5.1)

**PCI DSS V4-5.1.1** All security policies and operational procedures that are identified in Requirement 5 are:Documented.Kept up to date.In use.Known to all affected parties.

**Guidance:** Purpose: Requirement 5.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 5. While it is important to define the specific policies or procedures called out in Requirement 5, it is equally important to ensure they are properly documented, maintained, and disseminated. Good Practice: It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-5.1.2** Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.

**Guidance:** Purpose: If roles and responsibilities are not formally assigned, networks and systems may not be properly protected from malware. Good Practice: Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Malicious software (malware) is prevented, or detected and addressed.** (PCI DSS V4-5.2)

**PCI DSS V4-5.2.1** An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.

**Guidance:** Purpose: There is a constant stream of attacks targeting newly discovered vulnerabilities in systems previously regarded as secure. Without an anti- malware solution that is updated regularly, new forms of malware can be used to attack systems, disable a network, or compromise data. Good Practice: It is beneficial for entities to be aware of "zero- day" attacks (those that exploit a previously unknown vulnerability) and consider solutions that focus on behavioral characteristics and will alert and react to unexpected behavior.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-5.2.2** The deployed anti-malware solution(s):Detects all known types of malware.Removes, blocks, or contains all known types of malware.

**Guidance:** Purpose: It is important to protect against all types and forms of malware to prevent unauthorized access. Good Practice: Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning. Solution techniques include preventing malware from getting into the network and removing or containing

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-5.2.3** Any system components that are not at risk for malware are evaluated periodically to include the following:A documented list of all system components not at risk for malware.Identification and evaluation of evolving malware threats for those system components.Confirmation whether such system components continue to not require anti-malware protection.

**Guidance:** Purpose: Certain systems, at a given point in time, may not currently be commonly targeted or affected by malware. However, industry trends for malware can change quickly, so it is important for organizations to be aware of new malware that might affect their systems—for example, by monitoring vendor security notices and anti- malware forums to determine whether its systems might be coming under threat from new and evolving malware. Good Practice: If an entity determines that a particular system is not susceptible to any malware, the determination should be supported by industry evidence, vendor resources, and best practices. The following steps can help entities during their periodic evaluations: Identification of all system types previously determined to not require malware protection. Review of industry vulnerability alerts and notices to determine if new threats exist for any identified system. A documented conclusion about whether the system types remain not susceptible to malware. A strategy to add malware protection for any system types for which malware protection has become necessary. Trends in malware should be included in the identification of new security vulnerabilities at Requirement 6.3.1, and methods to address new trends should be incorporated into the entity’s configuration standards and protection mechanisms as needed.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-5.2.3.1** The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

**Guidance:** Purpose: Entities determine the optimum period to undertake the evaluation based on criteria such as the complexity of each entity’s environment and the number of types of systems that are required to be evaluated.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Monitor missing Endpoint Protection in Azure Security Center  
**Description:***Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Vulnerabilities in security configuration on your machines should be remediated  
**Description:***Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

## **Anti-malware mechanisms and processes are active, maintained, and monitored.** (PCI DSS V4-5.3)

**PCI DSS V4-5.3.1** The anti-malware solution(s) is kept current via automatic updates.

**Guidance:** Purpose: For an anti-malware solution to remain effective, it needs to have the latest security updates, signatures, threat analysis engines, and any other malware protections on which the solution relies. Having an automated update process avoids burdening end users with responsibility for manually installing updates and provides greater assurance that anti-malware protection mechanisms are updated as quickly as possible after an update is released. Good Practice: Anti-malware mechanisms should be updated via a trusted source as soon as possible after an update is available. Using a trusted common source to distribute updates to end-user systems helps ensure the integrity and consistency of the solution architecture. Updates may be automatically downloaded to a central location—for example, to allow for testing—prior to being deployed to individual system components.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-5.3.2** The anti-malware solution(s):Performs periodic scans and active or real-time scans.ORPerforms continuous behavioral analysis of systems or processes.

**Guidance:** Purpose: Periodic scans can identify malware that is present, but currently inactive, within the environment. Some malware, such as zero-day malware, can enter an environment before the scan solution is capable of detecting it. Performing regular periodic scans or continuous behavioral analysis of systems or processes helps ensure that previously undetectable malware can be identified, removed, and investigated to determine how it gained access to the environment. Good Practice: Using a combination of periodic scans (scheduled and on-demand) and active, real-time (on-access) scanning helps ensure that malware residing in both static and dynamic elements of the CDE is addressed. Users should also be able to run on- demand scans on their systems if suspicious activity is detected – this can be useful in the early detection of malware. Scans should include the entire file system, including all disks, memory, and start-up files and boot records (at system restart) to detect all malware upon file execution, including any software that may be resident on a system but not currently active. Scan scope should include all systems and software in the CDE, including those that are often overlooked such as email servers, web browsers, and instant messaging software.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-5.3.2.1** If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

**Guidance:** Purpose: Entities can determine the optimum period to undertake periodic scans based on their own assessment of the risks posed to their environments.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-5.3.3** For removable electronic media, the anti-malware solution(s):Performs automatic scans of when the media is inserted, connected, or logically mounted,ORPerforms continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.

**Guidance:** Purpose: Portable media devices are often overlooked as an entry method for malware. Attackers will often pre-load malware onto portable devices such as USB and flash drives; connecting an infected device to a computer then triggers the malware, introducing new threats within the environment.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-5.3.4** Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.

**Guidance:** Purpose: It is important to track the effectiveness of the anti-malware mechanisms—for example, by confirming that updates and scans are being performed as expected, and that malware is identified and addressed. Audit logs also allow an entity to determine how malware entered the environment and track its activity when inside the entity’s network.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-5.3.5** Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.

**Guidance:** Purpose: It is important that defensive mechanisms are always running so that malware is detected in real time. Ad-hoc starting and stopping of anti- malware solutions could allow malware to propagate unchecked and undetected. Good Practice: Where there is a legitimate need to temporarily disable a system’s anti-malware protection—for example, to support a specific maintenance activity or investigation of a technical problem— the reason for taking such action should be understood and approved by an appropriate management representative. Any disabling or altering of anti-malware mechanisms, including on administrators’ own devices, should be performed by authorized personnel. It is recognized that administrators have privileges that may allow them to disable anti-malware on their own computers, but there should be alerting mechanisms in place when such software is disabled and then follow up that occurs to ensure correct processes were followed.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Anti-phishing mechanisms protect users against phishing attacks.** (PCI DSS V4-5.4)

**PCI DSS V4-5.4.1** Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.

**Guidance:** Purpose: Technical controls can limit the number of occasions personnel have to evaluate the veracity of a communication and can also limit the effects of individual responses to phishing. Good Practice: When developing anti-phishing controls, entities are encouraged to consider a combination of approaches. For example, using anti-spoofing controls such as Domain-based Message Authentication, Reporting Conformance (DMARC), Sender Policy Framework (SPF), and Domain Keys Identified Mail (DKIM) will help stop phishers from spoofing the entity’s domain and impersonating personnel. The deployment of technologies for blocking phishing emails and malware before they reach personnel, such as link scrubbers and server-side anti-malware, can reduce incidents and decrease the time required by personnel to check and report phishing attacks. Additionally, training personnel to recognize and report phishing emails can allow similar emails to be identified and permit them to be removed before being opened. It is recommended (but not required) that anti- phishing controls are applied across an entity’s entire organization.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.** (PCI DSS V4-6.1)

**PCI DSS V4-6.1.1** All security policies and operational procedures that are identified in Requirement 6 are:Documented.Kept up to date.In use.Known to all affected parties.

**Guidance:** Purpose: Requirement 6.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 6. While it is important to define the specific policies or procedures called out in Requirement 6, it is equally important to ensure they are properly documented, maintained, and disseminated. Good Practice: It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.1.2** Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.

**Guidance:** Purpose: If roles and responsibilities are not formally assigned, systems will not be securely maintained, and their security level will be reduced. Good Practice: Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Bespoke and custom software are developed securely.** (PCI DSS V4-6.2)

**PCI DSS V4-6.2.1** Bespoke and custom software are developed securely, as follows: Based on industry standards and/or best practices for secure development.In accordance with PCI DSS (for example, secure authentication and logging).Incorporating consideration of information security issues during each stage of the software development lifecycle.

**Guidance:** Purpose: Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment. Good Practice: Understanding how sensitive data is handled by the application—including when stored, transmitted, and in memory—can help identify where data needs to be protected. PCI DSS requirements must be considered when developing software to meet those requirements by design, rather than trying to retrofit the software later.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.2.2** Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:On software security relevant to their job function and development languages.Including secure software design and secure coding techniques.Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

**Guidance:** Purpose: Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices. Good Practice: Training for developers may be provided in-house or by third parties. Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software. As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.2.3** Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: Code reviews ensure code is developed according to secure coding guidelines.Code reviews look for both existing and emerging software vulnerabilities.Appropriate corrections are implemented prior to release.

**Guidance:** Purpose: Security vulnerabilities in bespoke and custom software are commonly exploited by malicious individuals to gain access to a network and compromise account data. Vulnerable code is far more difficult and expensive to address after it has been deployed or released into production environments. Requiring a formal review and signoff by management prior to release helps to ensure that code is approved and has been developed in accordance with policies and procedures. Good Practice: The following items should be considered for inclusion in code reviews: Searching for undocumented features (implant tools, backdoors). Confirming that software securely uses external components’ functions (libraries, frameworks, APIs, etc.). For example, if a third-party library providing cryptographic functions is used, verify that it was integrated securely. Checking for correct use of logging to prevent sensitive data from getting into logs. Analysis of insecure code structures that may contain potential vulnerabilities related to common software attacks identified in Requirements 6.2.5. Checking the application’s behavior to detect logical vulnerabilities.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.2.3.1** If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.Reviewed and approved by management prior to release.

**Guidance:** Purpose: Having code reviewed by someone other than the original author, who is both experienced in code reviews and knowledgeable about secure coding practices, minimizes the possibility that code containing security or logic errors that could affect the security of cardholder data is released into a production environment. Requiring management approval that the code was reviewed limits the ability for the process to be bypassed. Good Practice: Having a formal review methodology and review checklists has been found to improve the quality of the code review process. Code review is a tiring process, and for this reason, it is most effective when reviewers only review small amounts of code at a time. To maintain the effectiveness of code reviews, it is beneficial to monitor the general workload of reviewers and to have them review applications they are familiar with. Code reviews may be performed using either manual or automated processes, or a combination of both. Entitles that rely solely on manual code review should ensure that reviewers maintain their skills through regular training as new vulnerabilities are found, and new secure coding methods are recommended.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.2.4** Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client- side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

**Guidance:** Purpose: Detecting or preventing common errors that result in vulnerable code as early as possible in the software development process lowers the probability that such errors make it through to production and lead to a compromise. Having formal engineering techniques and tools embedded in the development process will catch these errors early. This philosophy is sometimes called “shifting security left.” Good Practice: For both bespoke and custom software, the entity must ensure that code is developed focusing on the prevention or mitigation of common software attacks, including: Attempts to exploit common coding vulnerabilities (bugs) Attempts to exploit software design flaws. Attempts to exploit implementation/configuration flaws. Enumeration attacks – automated attacks that are actively exploited in payments and abuse identification, authentication, or authorization mechanisms. See the PCI Perspectives blog article “Beware of Account Testing Attacks.” Researching and documenting software engineering techniques or other methods helps to define how software developers prevent or mitigate various software attacks by features or countermeasures they build into software. This might include identification/authentication mechanisms, access control, input validation routines, etc. Developers should be familiar with different types of vulnerabilities and potential attacks and use measures to avoid potential attack vectors when developing code.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Secure transfer to storage accounts should be enabled  
**Description:***Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b encryption in transit enabled. | Ok |

**Parent** **Control:** Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources  
**Description:***Virtual machines without an enabled disk encryption will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that IAM users are not assigned the Service Account User or Service Account Token Creator roles at project level  
**Description:***It is recommended to assign the Service Account User (iam.serviceAccountUser) and Service Account Token Creator (iam.serviceAccountTokenCreator) roles to a user for a specific service account rather than assigning the role to a user at project level.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | No IAM users associated with iam.serviceAccountTokenCreator or iam.serviceAccountUser role. | Ok |

**Parent** **Control:** Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager  
**Description:***Google Cloud Functions allow you to host serverless code that is executed when an event is triggered, without the requiring the management a host operating system. These functions can also store environment variables to be used by the code that may contain authentication or other information that needs to remain confidential.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Separation of duties is enforced while assigning service account related roles to users  
**Description:***It is recommended that the principle of 'Separation of Duties' is enforced while assigning service-account related roles to users.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | mubashar@broadstonetech.com not assigned with both Service Account Admin and Service Account User roles. | Ok |
| **QA tester** | **Gcp** | bakarch.96@gmail.com not assigned with both Service Account Admin and Service Account User roles. | Ok |
| **QA tester** | **Gcp** | apps@cytex.io not assigned with both Service Account Admin and Service Account User roles. | Ok |
| **QA tester** | **Gcp** | umer@broadstonetech.com not assigned with both Service Account Admin and Service Account User roles. | Ok |

**Parent** **Control:** Ensure that Cloud Storage buckets have uniform bucket-level access enabled  
**Description:***It is recommended that uniform bucket-level access is enabled on Cloud Storage buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | cytex-85fe6.appspot.com uniform bucket-level access not enabled. | Alarm |
| **QA tester** | **Gcp** | staging.cytex-85fe6.appspot.com uniform bucket-level access not enabled. | Alarm |

**Parent** **Control:** Ensure that Separation of duties is enforced while assigning KMS related roles to users  
**Description:***It is recommended that the principle of 'Separation of Duties' is enforced while assigning KMS related roles to users.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | apps@cytex.io not assigned KMS admin and additional encrypter/decrypter roles. | Ok |
| **QA tester** | **Gcp** | bakarch.96@gmail.com not assigned KMS admin and additional encrypter/decrypter roles. | Ok |
| **QA tester** | **Gcp** | mubashar@broadstonetech.com not assigned KMS admin and additional encrypter/decrypter roles. | Ok |
| **QA tester** | **Gcp** | umer@broadstonetech.com not assigned KMS admin and additional encrypter/decrypter roles. | Ok |

**Parent** **Control:** Ensure that multi-factor authentication is enabled for all non-service accounts  
**Description:***Setup multi-factor authentication for Google Cloud Platform accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that dataproc cluster is encrypted using customer-managed encryption key  
**Description:***When you use Dataproc, cluster and job data is stored on Persistent Disks (PDs) associated with the Compute Engine VMs in your cluster and in a Cloud Storage staging bucket. This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Dataproc API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/dataproc.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/dataproc.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/cytex-85fe6"   "service": "dataproc.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Security Key Enforcement is enabled for all admin accounts  
**Description:***Setup Security Key Enforcement for Google Cloud Platform admin accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible  
**Description:***It is recommended that the IAM policy on Cloud KMS cryptokeys should restrict anonymous and/or public access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Key Management Service (KMS) API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "cloudkms.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Service Account has no Admin privileges  
**Description:***A service account is a special Google account that belongs to an application or a VM, instead of to an individual end-user. The application uses the service account to call the service's Google API so that users aren't directly involved. It's recommended not to use admin access for ServiceAccount.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | firebase-adminsdk has no admin privileges. | Ok |
| **QA tester** | **Gcp** | Steampipe CYTEX has no admin privileges. | Ok |
| **QA tester** | **Gcp** | Google-created service account App Engine default service account excluded. | Error |

**Parent** **Control:** Ensure user-managed/external keys for service accounts are rotated every 90 days or less  
**Description:***Service Account keys consist of a key ID (Private\_key\_Id) and Private key, which are used to sign programmatic requests users make to Google cloud services accessible to that particular service account. It is recommended that all Service Account keys are regularly rotated.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | firebase-adminsdk-1kgfn@cytex-85fe6.iam.gserviceaccount.com b1b6c3883426417f32f87f8ca39cd86fb7c8fa10 created 27-Oct-2020 (1043 days). | Alarm |
| **QA tester** | **Gcp** | steampipe-cytex@cytex-85fe6.iam.gserviceaccount.com 3641c86fbb9c7bd0fdbf3d87bb883aa73fc6f33f created 19-May-2023 (109 days). | Alarm |

**Parent** **Control:** Ensure API keys are restricted to use by only specified Hosts and Apps  
**Description:***Unrestricted 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 restrict API key usage to trusted hosts, HTTP referrers and apps.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure KMS encryption keys are rotated within a period of 90 days  
**Description:***Google Cloud Key Management Service stores cryptographic keys in a hierarchical structure designed for useful and elegant access control management. The format for the rotation schedule depends on the client library that is used. For the gcloud command-line tool, the next rotation time must be in ISO or RFC3339 format, and the rotation period must be in the form INTEGER[UNIT], where units can be one of seconds (s), minutes (m), hours (h) or days (d).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Key Management Service (KMS) API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "cloudkms.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure API keys are not created for a project  
**Description:***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 use standard authentication flow instead.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that there are only GCP-managed service account keys for each service account  
**Description:***User managed service accounts should not have user-managed keys.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | firebase-adminsdk has user-managed keys. | Alarm |
| **QA tester** | **Gcp** | Steampipe CYTEX has user-managed keys. | Alarm |
| **QA tester** | **Gcp** | App Engine default service account does not have user-managed keys. | Ok |

**Parent** **Control:** Ensure that Cloud Storage bucket is not anonymously or publicly accessible  
**Description:***It is recommended that IAM policy on Cloud Storage bucket does not allows anonymous or public access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | table 'gcp\_storage\_bucket' column 'iam\_policy' requires hydrate data from getGcpStorageBucketIAMPolicy  which failed with error googleapi: Error 403: steampipe-cytex@cytex-85fe6.iam.gserviceaccount.com does not have storage.buckets.getIamPolicy access to the Google Cloud Storage bucket. Permission 'storage.buckets.getIamPolicy' denied on resource (or it may not exist).  forbidden.  (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that corporate login credentials are used  
**Description:***Use corporate login credentials instead of personal accounts, such as Gmail accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | bakarch.96@gmail.com uses non-corporate login credentials. | Alarm |
| **QA tester** | **Gcp** | apps@cytex.io uses non-corporate login credentials. | Alarm |
| **QA tester** | **Gcp** | umer@broadstonetech.com uses non-corporate login credentials. | Alarm |
| **QA tester** | **Gcp** | mubashar@broadstonetech.com uses non-corporate login credentials. | Alarm |

**Parent** **Control:** Ensure API keys are restricted to only APIs that application needs access  
**Description:***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 restrict API keys to use (call) only APIs required by an application.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure API keys are rotated every 90 days  
**Description:***It is recommended to rotate API keys every 90 days.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

## **Security vulnerabilities are identified and addressed.** (PCI DSS V4-6.3)

**PCI DSS V4-6.3.1** Security vulnerabilities are identified and managed as follows:New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).Vulnerabilities are assigned a risk ranking based on industry best prRisk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

**Guidance:** Purpose: Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. Good Practice: Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. An organization’s processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.3.2** An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.

**Guidance:** Purpose: Identifying and listing all the entity’s bespoke and custom software, and any third-party software that is incorporated into the entity’s bespoke and custom software enables the entity to manage vulnerabilities and patches. Vulnerabilities in third-party components (including libraries, APIs, etc.) embedded in an entity’s software also renders those applications vulnerable to attacks. Knowing which third-party components are used in the entity’s software and monitoring the availability of security patches to address known vulnerabilities is critical to ensuring the security of the software. Good Practice: An entity’s inventory should cover all payment software components and dependencies, including supported execution platforms or environments, third-party libraries, services, and other required functionalities. There are many different types of solutions that can help with managing software inventories, such as software composition analysis tools, application discovery tools, and mobile device management.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.3.3** All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).

**Guidance:** Purpose: New exploits are constantly being discovered, and these can permit attacks against systems that have previously been considered secure. If the most recent security patches/updates are not implemented on critical systems as soon as possible, a malicious actor can use these exploits to attack or disable a system or gain access to sensitive data. Good Practice: Prioritizing security patches/updates for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. An entity’s patching cadence should factor in any re-evaluation of vulnerabilities and subsequent changes in the criticality of a vulnerability per Requirement 6.3.1. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities individually considered to be low or medium risk could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Monitor missing Endpoint Protection in Azure Security Center  
**Description:***Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Vulnerabilities in security configuration on your machines should be remediated  
**Description:***Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Prevent public users from having access to resources via IAM  
**Description:** *No description given.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | No public users have access to resources via IAM. | Ok |

**Parent** **Control:** Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects  
**Description:***For the virtual machines where you manage the operating system in Infrastructure as a Service (IaaS), you are responsible for keeping these operating systems and programs up to date. There are multiple ways to manage updates yourself that would be difficult to fit into one recommendation. Check the CIS Benchmarks for each of your Operating Systems as well for potential solutions there. In this recommendation we will use a feature in Google Cloud via its VM manager API to manage updates called Operating System Patch Management (referred to OS Patch Management from here on out). This may requires installing the OS Config API if it is not already installed. Also if you install custom operating systems, they may not functionally support the local OS config agent required to gather operating system patch information and issue update commands. These update commands are the default Linux and Windows commands to install updates such as yum or apt. This feature allows for a central management to issue those commands. OS Patch management also does not host the updates itself, so your VMs will need to be public or be able to access the internet. This is not the only Patch Management solution available to your organization and you should weigh your needs before committing to using this.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Check for open firewall rules allowing SSH from the internet  
**Description:** *No description given.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Check if service account keys are older than 100 days  
**Description:** *No description given.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | firebase-adminsdk-1kgfn@cytex-85fe6.iam.gserviceaccount.com b1b6c3883426417f32f87f8ca39cd86fb7c8fa10 created 27-Oct-2020 (1043 days). | Alarm |
| **QA tester** | **Gcp** | steampipe-cytex@cytex-85fe6.iam.gserviceaccount.com 3641c86fbb9c7bd0fdbf3d87bb883aa73fc6f33f created 19-May-2023 (109 days). | Alarm |
| **QA tester** | **Gcp** | firebase-adminsdk-1kgfn@cytex-85fe6.iam.gserviceaccount.com 24f57f5869f9fb7cf7a1211fea0d2fd935942b5b created 22-Aug-2023 (13 days). | Ok |
| **QA tester** | **Gcp** | firebase-adminsdk-1kgfn@cytex-85fe6.iam.gserviceaccount.com e3e58e9c850fd3985e6195842534ead3d1dde708 created 31-Aug-2023 (4 days). | Ok |
| **QA tester** | **Gcp** | cytex-85fe6@appspot.gserviceaccount.com f2ce99ee27e16fe1fc02023e0cabc0d31688dc37 created 31-Aug-2023 (4 days). | Ok |
| **QA tester** | **Gcp** | cytex-85fe6@appspot.gserviceaccount.com 16965dae07093dc0be6d80b708f6574129669a2d created 22-Aug-2023 (13 days). | Ok |
| **QA tester** | **Gcp** | steampipe-cytex@cytex-85fe6.iam.gserviceaccount.com 5d3740e89b4ef655a5d198b154598a2146608d04 created 22-Aug-2023 (13 days). | Ok |
| **QA tester** | **Gcp** | steampipe-cytex@cytex-85fe6.iam.gserviceaccount.com 9f0f58c78b140c7f5efcabc3deeffae546417e73 created 31-Aug-2023 (4 days). | Ok |

**Parent** **Control:** Check if Cloud SQL instances are world readable  
**Description:** *No description given.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Check for open firewall rules allowing TCP/UDP from the internet  
**Description:** *No description given.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Check that CMEK rotation policy is in place and is sufficiently short  
**Description:** *No description given.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Key Management Service (KMS) API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "cloudkms.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Only allow members from my domain to be added to IAM roles  
**Description:** *No description given.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | bakarch.96@gmail.com uses non-corporate login credentials. | Alarm |
| **QA tester** | **Gcp** | apps@cytex.io uses non-corporate login credentials. | Alarm |
| **QA tester** | **Gcp** | umer@broadstonetech.com uses non-corporate login credentials. | Alarm |
| **QA tester** | **Gcp** | mubashar@broadstonetech.com uses non-corporate login credentials. | Alarm |

## **Public-facing web applications are protected against attacks.** (PCI DSS V4-6.4)

**PCI DSS V4-6.4.1** For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:At least once every 12 months and after significant changes.By an entity that specializes in application security.Including, at a minimum, all common software attacks in Requirement 6.2.4.All vulnerabilities are ranked in accordance with requirement 6.3.1.All vulnerabilities are corrected.The application is re-evaluated after the correctionsOR Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:Installed in front of public-facing web applications to detect and prevent web- based attacks.Actively running and up to date as applicable.Generating audit logs.Configured to either block web-based attacks or generate an alert that is immediately investigated.

**Guidance:** Purpose: Public-facing web applications are those that are available to the public (not only for internal use). These applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. Good Practice: Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities. Common assessment tools include specialized web scanners that perform automatic analysis of web application protection. When using automated technical solutions, it is important to include processes that facilitate timely responses to alerts generated by the solutions so that any detected attacks can be mitigated.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.4.2** For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.Actively running and up to date as applicable.Generating audit logs.Configured to either block web-based attacks or generate an alert that is immediately investigated.

**Guidance:** Purpose: Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. Good Practice: When using automated technical solutions, it is important to include processes that facilitate timely responses to alerts generated by the solutions so that any detected attacks can be mitigated. Such solutions may also be used to automate mitigation, for example rate-limiting controls, which can be implemented to mitigate against brute-force attacks and enumeration attacks.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.4.3** All payment page scripts that are loaded and executed in the consumer’s browser are managed as follows: A method is implemented to confirm that each script is authorized.A method is implemented to assure the integrity of each script.An inventory of all scripts is maintained with written justification as to why each is necessary.

**Guidance:** Purpose: Scripts loaded and executed in the payment page can have their functionality altered without the entity’s knowledge and can also have the functionality to load additional external scripts (for example, advertising and tracking, tag management systems). Such seemingly harmless scripts can be used by potential attackers to upload malicious scripts that can read and exfiltrate cardholder data from the consumer browser. Ensuring that the functionality of all such scripts is understood to be necessary for the operation of the payment page minimizes the number of scripts that could be tampered with. Ensuring that scripts have been explicitly authorized reduces the probability of unnecessary scripts being added to the payment page without appropriate management approval. Using techniques to prevent tampering with the script will minimize the probability of the script being modified to carry out unauthorized behavior, such as skimming the cardholder data from the payment page. Good Practice: Scripts may be authorized by manual or automated (e.g., workflow) processes. Where the payment page will be loaded into an inline frame (IFRAME), restricting the location that the payment page can be loaded from, using the parent page’s Content Security Policy (CSP) can help prevent unauthorized content being substituted for the payment page.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** WAF regional rule should have at least one condition  
**Description:***This control checks whether WAF regional rule contains any conditions. The control fails if no conditions are present within a rule.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error WAF Regional: ListRules  https response error StatusCode: 400  RequestID: ab133cee-1089-4fb9-b296-bf1bb4c354df  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: waf-regional:ListRules on resource: arn:aws:waf-regional:us-east-1:986601184113:rule/\* because no identity-based policy allows the waf-regional:ListRules action (SQLSTATE HV000) | Error |

**Parent** **Control:** WAF global rule should have at least one condition  
**Description:***This control checks whether an AWS WAF global rule contains any conditions. The control fails if no conditions are present within a rule.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error WAF: ListRules  https response error StatusCode: 400  RequestID: 4af13c7a-d050-40be-a1b8-34f694b61102  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: waf:ListRules on resource: arn:aws:waf::986601184113:rule/\* because no identity-based policy allows the waf:ListRules action (SQLSTATE HV000) | Error |

**Parent** **Control:** API Gateway stage should be associated with waf  
**Description:***Ensure if an Amazon API Gateway API stage is using a WAF Web ACL. This rule is non compliant if an AWS WAF Web ACL is not used.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | beta not associated with WAF web ACL. | Alarm |

**Parent** **Control:** WAF global rule group should have at least one rule  
**Description:***This control checks whether WAF global rule group has at least one rule. The control fails if no rules are present within a rule group.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error WAF: ListRuleGroups  https response error StatusCode: 400  RequestID: b1aa7c4a-c69d-4edd-811c-167a1c818cfb  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: waf:ListRuleGroups on resource: arn:aws:waf::986601184113:rulegroup/\* because no identity-based policy allows the waf:ListRuleGroups action (SQLSTATE HV000) | Error |

**Parent** **Control:** Monitor missing Endpoint Protection in Azure Security Center  
**Description:***Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Vulnerabilities in security configuration on your machines should be remediated  
**Description:***Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. Check control description for more details. | Manual |

**Parent** **Control:** Ensure that VPC Flow Logs is enabled for every subnet in a VPC Network  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Cloud Storage buckets have uniform bucket-level access enabled  
**Description:***It is recommended that uniform bucket-level access is enabled on Cloud Storage buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | cytex-85fe6.appspot.com uniform bucket-level access not enabled. | Alarm |
| **QA tester** | **Gcp** | staging.cytex-85fe6.appspot.com uniform bucket-level access not enabled. | Alarm |

**Parent** **Control:** Ensure no HTTPS or SSL proxy load balancers permit SSL policies with weak cipher suites  
**Description:***Secure Sockets Layer (SSL) policies determine what port Transport Layer Security (TLS) features clients are permitted to use when connecting to load balancers.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Cloud Storage bucket is not anonymously or publicly accessible  
**Description:***It is recommended that IAM policy on Cloud Storage bucket does not allows anonymous or public access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | table 'gcp\_storage\_bucket' column 'iam\_policy' requires hydrate data from getGcpStorageBucketIAMPolicy  which failed with error googleapi: Error 403: steampipe-cytex@cytex-85fe6.iam.gserviceaccount.com does not have storage.buckets.getIamPolicy access to the Google Cloud Storage bucket. Permission 'storage.buckets.getIamPolicy' denied on resource (or it may not exist).  forbidden.  (SQLSTATE HV000) | Error |

## **Changes to all system components are managed securely.** (PCI DSS V4-6.5)

**PCI DSS V4-6.5.1** Changes to all system components in the production environment are made according to established procedures that include: Reason for, and description of, the changeDocumentation of security impact.Documented change approval by authorized parties.Testing to verify that the change does not adversely impact system security.For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.Procedures to address failures and return to a secure state.

**Guidance:** Purpose: Change management procedures must be applied to all changes—including the addition, removal, or modification of any system component—in the production environment. It is important to document the reason for a change and the change description so that relevant parties understand and agree the change is needed. Likewise, documenting the impacts of the change allows all affected parties to plan appropriately for any processing changes. Good Practice: Approval by authorized parties confirms that the change is legitimate and that the change is sanctioned by the organization. Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Thorough testing by the entity confirms that the security of the environment is not reduced by implementing a change and that all existing security controls either remain in place or are replaced with equal or stronger security controls after the change. The specific testing to be performed will vary according to the type of change and system component(s) affected. For each change, it is important to have documented procedures that address any failures and provide instructions on how to return to a secure state in case the change fails or adversely affects the security of an application or system. These procedures will allow the application or system to be restored to its previous secure state.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.5.2** Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

**Guidance:** Purpose: Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment, and that PCI DSS requirements continue to be met to secure the environment. Good Practice: Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.5.3** Pre-production environments are separated from production environments and the separation is enforced with access controls.

**Guidance:** Purpose: Due to the constantly changing state of pre- production environments, they are often less secure than the production environment. Good Practice: Organizations must clearly understand which environments are test environments or development environments and how these environments interact on the level of networks and applications.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.5.4** Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.

**Guidance:** Purpose: The goal of separating roles and functions between production and pre-production environments is to reduce the number of personnel with access to the production environment and account data and thereby minimize risk of unauthorized, unintentional, or inappropriate access to data and system components and help ensure that access is limited to those individuals with a business need for such access. The intent of this control is to separate critical activities to provide oversight and review to catch errors and minimize the chances of fraud or theft (since two people would need to collude in order to hide an activity). Separating roles and functions, also referred to as separation or segregation of duties, is a key internal control concept to protect an entity’s assets.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.5.5** Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.

**Guidance:** Purpose: Use of live PANs outside of protected CDEs provides malicious individuals with the opportunity to gain unauthorized access to cardholder data. Good Practice: Entities can minimize their storage of live PANs by only storing them in pre-production when strictly necessary for a specific and defined testing purpose and securely deleting that data after use. If an entity requires PANs specifically designed for test purposes, these can be obtained from acquirers.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**PCI DSS V4-6.5.6** Test data and test accounts are removed from system components before the system goes into production.

**Guidance:** Purpose: This data may give away information about the functioning of an application or system and is an easy target for unauthorized individuals to exploit to gain access to systems. Possession of such information could facilitate compromise of the system and related account data.

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Ensure that IAM users are not assigned the Service Account User or Service Account Token Creator roles at project level  
**Description:***It is recommended to assign the Service Account User (iam.serviceAccountUser) and Service Account Token Creator (iam.serviceAccountTokenCreator) roles to a user for a specific service account rather than assigning the role to a user at project level.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | No IAM users associated with iam.serviceAccountTokenCreator or iam.serviceAccountUser role. | Ok |

**Parent** **Control:** Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager  
**Description:***Google Cloud Functions allow you to host serverless code that is executed when an event is triggered, without the requiring the management a host operating system. These functions can also store environment variables to be used by the code that may contain authentication or other information that needs to remain confidential.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Security Key Enforcement is enabled for all admin accounts  
**Description:***Setup Security Key Enforcement for Google Cloud Platform admin accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that corporate login credentials are used  
**Description:***Use corporate login credentials instead of personal accounts, such as Gmail accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | bakarch.96@gmail.com uses non-corporate login credentials. | Alarm |
| **QA tester** | **Gcp** | apps@cytex.io uses non-corporate login credentials. | Alarm |
| **QA tester** | **Gcp** | umer@broadstonetech.com uses non-corporate login credentials. | Alarm |
| **QA tester** | **Gcp** | mubashar@broadstonetech.com uses non-corporate login credentials. | Alarm |

**Parent** **Control:** Ensure that there are only GCP-managed service account keys for each service account  
**Description:***User managed service accounts should not have user-managed keys.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | firebase-adminsdk has user-managed keys. | Alarm |
| **QA tester** | **Gcp** | Steampipe CYTEX has user-managed keys. | Alarm |
| **QA tester** | **Gcp** | App Engine default service account does not have user-managed keys. | Ok |

**Parent** **Control:** Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible  
**Description:***It is recommended that the IAM policy on Cloud KMS cryptokeys should restrict anonymous and/or public access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Key Management Service (KMS) API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "cloudkms.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure KMS encryption keys are rotated within a period of 90 days  
**Description:***Google Cloud Key Management Service stores cryptographic keys in a hierarchical structure designed for useful and elegant access control management. The format for the rotation schedule depends on the client library that is used. For the gcloud command-line tool, the next rotation time must be in ISO or RFC3339 format, and the rotation period must be in the form INTEGER[UNIT], where units can be one of seconds (s), minutes (m), hours (h) or days (d).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Key Management Service (KMS) API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "cloudkms.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure API keys are not created for a project  
**Description:***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 use standard authentication flow instead.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Service Account has no Admin privileges  
**Description:***A service account is a special Google account that belongs to an application or a VM, instead of to an individual end-user. The application uses the service account to call the service's Google API so that users aren't directly involved. It's recommended not to use admin access for ServiceAccount.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | firebase-adminsdk has no admin privileges. | Ok |
| **QA tester** | **Gcp** | Steampipe CYTEX has no admin privileges. | Ok |
| **QA tester** | **Gcp** | Google-created service account App Engine default service account excluded. | Error |

**Parent** **Control:** Ensure that Separation of duties is enforced while assigning service account related roles to users  
**Description:***It is recommended that the principle of 'Separation of Duties' is enforced while assigning service-account related roles to users.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | mubashar@broadstonetech.com not assigned with both Service Account Admin and Service Account User roles. | Ok |
| **QA tester** | **Gcp** | bakarch.96@gmail.com not assigned with both Service Account Admin and Service Account User roles. | Ok |
| **QA tester** | **Gcp** | apps@cytex.io not assigned with both Service Account Admin and Service Account User roles. | Ok |
| **QA tester** | **Gcp** | umer@broadstonetech.com not assigned with both Service Account Admin and Service Account User roles. | Ok |

**Parent** **Control:** Ensure API keys are restricted to only APIs that application needs access  
**Description:***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 restrict API keys to use (call) only APIs required by an application.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Separation of duties is enforced while assigning KMS related roles to users  
**Description:***It is recommended that the principle of 'Separation of Duties' is enforced while assigning KMS related roles to users.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | apps@cytex.io not assigned KMS admin and additional encrypter/decrypter roles. | Ok |
| **QA tester** | **Gcp** | bakarch.96@gmail.com not assigned KMS admin and additional encrypter/decrypter roles. | Ok |
| **QA tester** | **Gcp** | mubashar@broadstonetech.com not assigned KMS admin and additional encrypter/decrypter roles. | Ok |
| **QA tester** | **Gcp** | umer@broadstonetech.com not assigned KMS admin and additional encrypter/decrypter roles. | Ok |

**Parent** **Control:** Ensure user-managed/external keys for service accounts are rotated every 90 days or less  
**Description:***Service Account keys consist of a key ID (Private\_key\_Id) and Private key, which are used to sign programmatic requests users make to Google cloud services accessible to that particular service account. It is recommended that all Service Account keys are regularly rotated.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | firebase-adminsdk-1kgfn@cytex-85fe6.iam.gserviceaccount.com b1b6c3883426417f32f87f8ca39cd86fb7c8fa10 created 27-Oct-2020 (1043 days). | Alarm |
| **QA tester** | **Gcp** | steampipe-cytex@cytex-85fe6.iam.gserviceaccount.com 3641c86fbb9c7bd0fdbf3d87bb883aa73fc6f33f created 19-May-2023 (109 days). | Alarm |

**Parent** **Control:** Ensure that multi-factor authentication is enabled for all non-service accounts  
**Description:***Setup multi-factor authentication for Google Cloud Platform accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure API keys are restricted to use by only specified Hosts and Apps  
**Description:***Unrestricted 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 restrict API key usage to trusted hosts, HTTP referrers and apps.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure API keys are rotated every 90 days  
**Description:***It is recommended to rotate API keys every 90 days.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that dataproc cluster is encrypted using customer-managed encryption key  
**Description:***When you use Dataproc, cluster and job data is stored on Persistent Disks (PDs) associated with the Compute Engine VMs in your cluster and in a Cloud Storage staging bucket. This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Dataproc API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/dataproc.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/dataproc.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/cytex-85fe6"   "service": "dataproc.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

# System Operations

## **Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.** (NIST-PR.AC)

**NIST-PR.AC.1** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AC.2** Physical access to assets is managed and protected

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AC.3** Remote access is managed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AC.4** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AC.5** Network integrity is protected, incorporating network segregation where appropriate

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AC.6** Identities are proofed and bound to credentials, and asserted in interactions when appropriate

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AC.7** Users, devices, and other assets are authenticated (e.g., single.factor, multi.factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** VPC security groups should restrict ingress TCP and UDP access from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a does not allow ingress to TCP or UDP ports from 0.0.0.0/0. | Ok |

**Parent** **Control:** IAM password policies for users should have strong configurations  
**Description:***The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Strong password policies not configured. | Alarm |

**Parent** **Control:** IAM root user should not have access keys  
**Description:***Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No root user access keys exist. | Ok |

**Parent** **Control:** VPC internet gateways should be attached to authorized vpc  
**Description:***Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | igw-f1468595 attached to vpc-db2853b. | Ok |

**Parent** **Control:** IAM user credentials that have not been used in 90 days should be disabled  
**Description:***AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex password not enabled  key 1 created 06-Jan-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | cytexaudit password not enabled  key 1 created 02-Mar-2022 never used  key 2 used 01-Sep-2023. | Alarm |
| **qa tester** | **AWS** | farrukh password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | jediar password used 31-Aug-2023  key 1 created 04-Mar-2022 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | prytex password not enabled  key 1 used 26-Aug-2020  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | s3readonly password not enabled  key 1 used 12-Oct-2020  key 2 used 05-Jul-2023. | Alarm |
| **qa tester** | **AWS** | taimur password used 17-Jun-2021  key 1 created 16-Jun-2021 never used  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | testcytex password used 29-Nov-2021  key 1 not enabled  key 2 not enabled. | Alarm |
| **qa tester** | **AWS** | root\_account password used 10-Jul-2023  key 1 not enabled  key 2 not enabled. | Error |

**Parent** **Control:** IAM user access keys should be rotated at least every 90 days  
**Description:***The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit AKIA6LNQDLNY2UXNZV4Z created 08-Mar-2022 (541 days). | Alarm |
| **qa tester** | **AWS** | cytexaudit AKIA6LNQDLNY5RKMW5YO created 02-Mar-2022 (547 days). | Alarm |
| **qa tester** | **AWS** | jediar AKIA6LNQDLNYQFEAZJFV created 04-Mar-2022 (546 days). | Alarm |
| **qa tester** | **AWS** | prytex AKIA6LNQDLNYQVA7ZH3U created 25-Aug-2020 (1102 days). | Alarm |
| **qa tester** | **AWS** | s3readonly AKIA6LNQDLNYWEAOKYJT created 08-Mar-2022 (541 days). | Alarm |
| **qa tester** | **AWS** | s3readonly AKIA6LNQDLNYRYRZ4OFT created 07-Oct-2020 (1059 days). | Alarm |
| **qa tester** | **AWS** | cytex AKIA6LNQDLNY2O4WV57L created 06-Jan-2022 (603 days). | Alarm |
| **qa tester** | **AWS** | farrukh AKIA6LNQDLNYZTDD3WXR created 16-Jun-2021 (807 days). | Alarm |
| **qa tester** | **AWS** | taimur AKIA6LNQDLNYSKL4WSF3 created 16-Jun-2021 (807 days). | Alarm |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** IAM users with console access should have MFA enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testcytex password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | jediar password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | taimur password login enabled but no MFA device configured. | Alarm |
| **qa tester** | **AWS** | root\_account password login enabled and MFA device configured. | Ok |
| **qa tester** | **AWS** | cytex password login disabled. | Ok |
| **qa tester** | **AWS** | cytexaudit password login disabled. | Ok |
| **qa tester** | **AWS** | farrukh password login enabled and MFA device configured. | Ok |
| **qa tester** | **AWS** | prytex password login disabled. | Ok |
| **qa tester** | **AWS** | s3readonly password login disabled. | Ok |

**Parent** **Control:** IAM user MFA should be enabled  
**Description:***Enable this rule to restrict access to resources in the AWS Cloud.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | cytexaudit MFA device not configured. | Alarm |
| **qa tester** | **AWS** | jediar MFA device not configured. | Alarm |
| **qa tester** | **AWS** | prytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | s3readonly MFA device not configured. | Alarm |
| **qa tester** | **AWS** | taimur MFA device not configured. | Alarm |
| **qa tester** | **AWS** | testcytex MFA device not configured. | Alarm |
| **qa tester** | **AWS** | root\_account MFA device configured. | Ok |
| **qa tester** | **AWS** | farrukh MFA device configured. | Ok |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** VPC default security group should not allow inbound and outbound traffic  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Default security group sg-7344060a has inbound and outbound rules. | Alarm |

**Parent** **Control:** IAM root user MFA should be enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | MFA enabled for root account. | Ok |

**Parent** **Control:** IAM policy should not have statements with admin access  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing 'Effect': 'Allow' with 'Action': '\*' over 'Resource': '\*'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | AWSLambdaEdgeExecutionRole-adc0e8e5-65d9-40a5-aaff-752d94f98e81 contains 0 statements that allow action "\*" on resource "\*". | Ok |
| **qa tester** | **AWS** | cytexaudit\_sploit contains 0 statements that allow action "\*" on resource "\*". | Ok |

**Parent** **Control:** IAM groups should have at least one user  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | developers associated with IAM user. | Ok |
| **qa tester** | **AWS** | Group\_S3 associated with IAM user. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM user. | Ok |
| **qa tester** | **AWS** | ar\_dev associated with IAM user. | Ok |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** IAM user should not have any inline or attached policies  
**Description:***This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | cytexaudit has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | jediar has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | s3readonly has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | taimur has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | testcytex has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | farrukh has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | prytex has 0 inline and 0 directly attached policies. | Ok |

**Parent** **Control:** VPC security groups should restrict ingress access on ports 20, 21, 22, 3306, 3389, 4333 from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for ports 20  21  22  3306  3389  4333 from 0.0.0.0/0. | Ok |

**Parent** **Control:** VPC security groups should restrict ingress SSH access from 0.0.0.0/0  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for SSH from 0.0.0.0/0. | Ok |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** IAM users should be in at least one group  
**Description:***AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytexaudit not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | s3readonly not associated with any IAM group. | Alarm |
| **qa tester** | **AWS** | taimur associated with IAM group. | Ok |
| **qa tester** | **AWS** | cytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | jediar associated with IAM group. | Ok |
| **qa tester** | **AWS** | prytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | testcytex associated with IAM group. | Ok |
| **qa tester** | **AWS** | farrukh associated with IAM group. | Ok |

**Parent** **Control:** IAM root user hardware MFA should be enabled  
**Description:***Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | MFA enabled for root account  but the MFA associated is a virtual device. | Alarm |

**Parent** **Control:** Lambda functions should be in a VPC  
**Description:***Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test is not in VPC. | Alarm |
| **qa tester** | **AWS** | trap\_doors\_lambda is not in VPC. | Alarm |
| **qa tester** | **AWS** | escapeRoomLambdaFunc is not in VPC. | Alarm |
| **qa tester** | **AWS** | esportsgps is not in VPC. | Alarm |
| **qa tester** | **AWS** | medical\_care is not in VPC. | Alarm |

**Parent** **Control:** Ensure a Custom Role is Assigned Permissions for Administering Resource Locks  
**Description:***Resource locking is a powerful protection mechanism that can prevent inadvertent modification/deletion of resources within Azure subscriptions/Resource Groups and is a recommended NIST configuration.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'  
**Description:***Limit guest user permissions.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access  
**Description:***Some Azure services that interact with storage accounts operate from networks that can't be granted access through network rules. To help this type of service work as intended, allow the set of trusted Azure services to bypass the network rules. These services will then use strong authentication to access the storage account. If the Allow trusted Azure services exception is enabled, the following services are granted access to the storage account: Azure Backup, Azure Site Recovery, Azure DevTest Labs, Azure Event Grid, Azure Event Hubs, Azure Networking, Azure Monitor, and Azure SQL Data Warehouse (when registered in the subscription).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b trusted Microsoft services enabled. | Ok |

**Parent** **Control:** Ensure that Resource Locks are set for Mission-Critical Azure Resources  
**Description:***Resource Manager Locks provide a way for administrators to lock down Azure resources to prevent deletion of, or modifications to, a resource. These locks sit outside of the Role Based Access Controls (RBAC) hierarchy and, when applied, will place restrictions on the resource for all users. These locks are very useful when there is an important resource in a subscription that users should not be able to delete or change. Locks can help prevent accidental and malicious changes or deletion.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Access Review is Set Up for External Users in Azure AD Privileged Identity Management  
**Description:***This recommendation extends guest access review by utilizing the Azure AD Privileged Identity Management feature provided in Azure AD Premium P2. Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data. Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources a a guest user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Guest Users Are Reviewed on a Regular Basis  
**Description:***Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data. Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources as a guest user. Guest users in every subscription should be review on a regular basis to ensure that inactive and unneeded accounts are removed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes'  
**Description:***Ensure that all administrators are notified if any other administrator resets their password.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That 'Restrict access to Azure AD administration portal' is Set to 'Yes'  
**Description:***Restrict access to the Azure AD administration portal to administrators only.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That ‘Subscription Entering AAD Directory’ and ‘Subscription Leaving AAD Directory’ Is Set To ‘Permit No One’  
**Description:***Users who are set as subscription owners are able to make administrative changes to the subscriptions and move them into and out of Azure Active Directories.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That ‘Users Can Consent to Apps Accessing Company Data on Their Behalf’ Is Set To ‘Allow for Verified Publishers’  
**Description:***Allow users to provide consent for selected permissions when a request is coming from a verified publisher.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No'  
**Description:***Require administrators to provide consent for the apps before use.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'  
**Description:***Restrict invitations to users with specific administrative roles only.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Number of days before users are asked to reconfirm their authentication information' is not set to '0'  
**Description:***Ensure that the number of days before users are asked to re-confirm their authentication information is not set to 0.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Storage Account Access Keys are Periodically Regenerated  
**Description:***For increased security, regenerate storage account access keys periodically.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Shared Access Signature Tokens Expire Within an Hour  
**Description:***Expire shared access signature tokens within an hour.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services  
**Description:***Automatic Key Rotation is available in Public Preview. The currently supported applications are Key Vault, Managed Disks, and Storage accounts accessing keys within Key Vault. The number of supported applications will incrementally increased.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Trusted Locations Are Defined  
**Description:***Azure Active Directory Conditional Access allows an organization to configure Named locations and configure whether those locations are trusted or untrusted. These settings provide organizations the means to specify Geographical locations for use in conditional access policies, or define actual IP addresses and IP ranges and whether or not those IP addresses and/or ranges are trusted by the organization.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Default Network Access Rule for Storage Accounts is Set to Deny  
**Description:***Restricting default network access helps to provide a new layer of security, since storage accounts accept connections from clients on any network. To limit access to selected networks, the default action must be changed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b allows traffic from all networks. | Alarm |

**Parent** **Control:** Ensure Private Endpoints are used to access Storage Accounts  
**Description:***Use private endpoints for your Azure Storage accounts to allow clients and services to securely access data located over a network via an encrypted Private Link. To do this, the private endpoint uses an IP address from the VNet for each service. Network traffic between disparate services securely traverses encrypted over the VNet. This VNet can also link addressing space, extending your network and accessing resources on it. Similarly, it can be a tunnel through public networks to connect remote infrastructures together. This creates further security through segmenting network traffic and preventing outside sources from accessing it.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not uses private link. | Alarm |

**Parent** **Control:** Ensure that Network Watcher is 'Enabled'  
**Description:***Enable Network Watcher for Azure subscriptions.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in polandcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in jioindiawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaecentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japaneast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in francesouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in qatarcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in switzerlandnorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwaywest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in swedencentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westus3. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uaenorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in japanwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricanorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westeurope. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southafricawest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanynorth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southeastasia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in eastus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in northcentralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiasoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in ukwest. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreasouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in centralus. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in brazilsoutheast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in canadaeast. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in westindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in uksouth. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in southindia. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in koreacentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in australiacentral2. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in germanywestcentral. | Alarm |
| **SQAE** | **Azure** | Network watcher not enabled in norwayeast. | Alarm |

**Parent** **Control:** Ensure that IAM users are not assigned the Service Account User or Service Account Token Creator roles at project level  
**Description:***It is recommended to assign the Service Account User (iam.serviceAccountUser) and Service Account Token Creator (iam.serviceAccountTokenCreator) roles to a user for a specific service account rather than assigning the role to a user at project level.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | No IAM users associated with iam.serviceAccountTokenCreator or iam.serviceAccountUser role. | Ok |

**Parent** **Control:** Ensure that Separation of duties is enforced while assigning service account related roles to users  
**Description:***It is recommended that the principle of 'Separation of Duties' is enforced while assigning service-account related roles to users.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | mubashar@broadstonetech.com not assigned with both Service Account Admin and Service Account User roles. | Ok |
| **QA tester** | **Gcp** | bakarch.96@gmail.com not assigned with both Service Account Admin and Service Account User roles. | Ok |
| **QA tester** | **Gcp** | apps@cytex.io not assigned with both Service Account Admin and Service Account User roles. | Ok |
| **QA tester** | **Gcp** | umer@broadstonetech.com not assigned with both Service Account Admin and Service Account User roles. | Ok |

**Parent** **Control:** Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible  
**Description:***It is recommended that the IAM policy on Cloud KMS cryptokeys should restrict anonymous and/or public access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Key Management Service (KMS) API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "cloudkms.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Separation of duties is enforced while assigning KMS related roles to users  
**Description:***It is recommended that the principle of 'Separation of Duties' is enforced while assigning KMS related roles to users.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | apps@cytex.io not assigned KMS admin and additional encrypter/decrypter roles. | Ok |
| **QA tester** | **Gcp** | bakarch.96@gmail.com not assigned KMS admin and additional encrypter/decrypter roles. | Ok |
| **QA tester** | **Gcp** | mubashar@broadstonetech.com not assigned KMS admin and additional encrypter/decrypter roles. | Ok |
| **QA tester** | **Gcp** | umer@broadstonetech.com not assigned KMS admin and additional encrypter/decrypter roles. | Ok |

**Parent** **Control:** Ensure 'Access Approval' is 'Enabled'  
**Description:***GCP Access Approval enables you to require your organizations' explicit approval whenever Google support try to access your projects. You can then select users within your organization who can approve these requests through giving them a security role in IAM. All access requests display which Google Employee requested them in an email or Pub/Sub message that you can choose to Approve. This adds an additional control and logging of who in your organization approved/denied these requests.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | table 'gcp\_project' column 'access\_approval\_settings' requires hydrate data from getProjectAccessApprovalSettings  which failed with error googleapi: Error 403: Access Approval API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/accessapproval.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/accessapproval.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "accessapproval.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured.  (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Compute instances do not have public IP addresses  
**Description:***Compute instances should not be configured to have external IP addresses.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Cloud Storage bucket is not anonymously or publicly accessible  
**Description:***It is recommended that IAM policy on Cloud Storage bucket does not allows anonymous or public access.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | table 'gcp\_storage\_bucket' column 'iam\_policy' requires hydrate data from getGcpStorageBucketIAMPolicy  which failed with error googleapi: Error 403: steampipe-cytex@cytex-85fe6.iam.gserviceaccount.com does not have storage.buckets.getIamPolicy access to the Google Cloud Storage bucket. Permission 'storage.buckets.getIamPolicy' denied on resource (or it may not exist).  forbidden.  (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Cloud Storage buckets have uniform bucket-level access enabled  
**Description:***It is recommended that uniform bucket-level access is enabled on Cloud Storage buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | cytex-85fe6.appspot.com uniform bucket-level access not enabled. | Alarm |
| **QA tester** | **Gcp** | staging.cytex-85fe6.appspot.com uniform bucket-level access not enabled. | Alarm |

**Parent** **Control:** Ensure 'skip\_show\_database' database flag for Cloud SQL Mysql instance is set to 'on'  
**Description:***It is recommended to set skip\_show\_database database flag for Cloud SQL Mysql instance to on.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'  
**Description:***It is recommended to set cross db ownership chaining database flag for Cloud SQL SQL Server instance to off.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off'  
**Description:***It is recommended to set contained database authentication database flag for Cloud SQL on the SQL Server instance is set to off.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses  
**Description:***Database Server should accept connections only from trusted Network(s)/IP(s) and restrict access from public IP addresses.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Cloud SQL database instances do not have public IPs  
**Description:***It is recommended to configure Second Generation Sql instance to use private IPs instead of public IPs.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that instances are not configured to use the default service account  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that instances are not configured to use the default service account with full access to all Cloud APIs  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that a MySQL database instance does not allow anyone to connect with administrative privileges  
**Description:***It is recommended to set a password for the administrative user (root by default) to prevent unauthorized access to the SQL database instances. This recommendation is applicable only for MySQL Instances. PostgreSQL does not offer any setting for No Password from the cloud console.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that there are only GCP-managed service account keys for each service account  
**Description:***User managed service accounts should not have user-managed keys.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | firebase-adminsdk has user-managed keys. | Alarm |
| **QA tester** | **Gcp** | Steampipe CYTEX has user-managed keys. | Alarm |
| **QA tester** | **Gcp** | App Engine default service account does not have user-managed keys. | Ok |

**Parent** **Control:** Ensure that multi-factor authentication is enabled for all non-service accounts  
**Description:***Setup multi-factor authentication for Google Cloud Platform accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Security Key Enforcement is enabled for all admin accounts  
**Description:***Setup Security Key Enforcement for Google Cloud Platform admin accounts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Cloud Asset Inventory Is Enabled  
**Description:***GCP Cloud Asset Inventory is services that provides a historical view of GCP resources and IAM policies through a time-series database. The information recorded includes metadata on Google Cloud resources, metadata on policies set on Google Cloud projects or resources, and runtime information gathered within a Google Cloud resource.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | cloudasset.googleapis.com Cloud Asset API is disabled. | Alarm |

**Parent** **Control:** Ensure oslogin is enabled for a Project  
**Description:***Enabling OS login binds SSH certificates to IAM users and facilitates effective SSH certificate management.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

## **Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurityrelated duties and responsibilities consistent with related policies, procedures, and agreements.** (NIST-PR.AT)

**NIST-PR.AT.1** All users are informed and trained

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AT.2** Privileged users understand roles and responsibilities

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AT.3** Third.party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AT.4** Senior executives understand roles and responsibilities

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.AT.5** Physical and information security personnel understand roles and responsibilities

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Ensure that Compute instances have Confidential Computing enabled  
**Description:***Google Cloud encrypts data at-rest and in-transit, but customer data must be decrypted for processing. Confidential Computing is a breakthrough technology which encrypts data in-use—while it is being processed. Confidential Computing environments keep data encrypted in memory and elsewhere outside the central processing unit (CPU).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

## **Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.** (NIST-PR.DS)

**NIST-PR.DS.1** Data.at.rest is protected

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.DS.2** Data.in.transit is protected

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.DS.3** Assets are formally managed throughout removal, transfers, and disposition

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.DS.4** Adequate capacity to ensure availability is maintained

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.DS.5** Protections against data leaks are implemented

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.DS.6** Integrity checking mechanisms are used to verify software, firmware, and information integrity

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.DS.7** The development and testing environment(s) are separate from the production environment

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.DS.8** Integrity checking mechanisms are used to verify hardware integrity

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** GuardDuty should be enabled  
**Description:***Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** VPC security groups should be associated with at least one ENI  
**Description:***This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | default not associated to any ENI. | Alarm |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** API Gateway stage cache encryption at rest should be enabled  
**Description:***To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | beta API cache and encryption not enabled. | Alarm |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** SNS topics should be encrypted at rest  
**Description:***To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | dynamodb encryption at rest disabled. | Alarm |

**Parent** **Control:** S3 bucket default encryption should be enabled  
**Description:***To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | usdztestingbucket default encryption enabled. | Ok |
| **qa tester** | **AWS** | cytex default encryption enabled. | Ok |
| **qa tester** | **AWS** | prytex default encryption enabled. | Ok |
| **qa tester** | **AWS** | edmsnapshots default encryption enabled. | Ok |
| **qa tester** | **AWS** | devicedetector default encryption enabled. | Ok |
| **qa tester** | **AWS** | bstfintech default encryption enabled. | Ok |
| **qa tester** | **AWS** | bstlegal default encryption enabled. | Ok |
| **qa tester** | **AWS** | entjedi default encryption enabled. | Ok |
| **qa tester** | **AWS** | jediar default encryption enabled. | Ok |
| **qa tester** | **AWS** | testing177 default encryption enabled. | Ok |

**Parent** **Control:** S3 bucket object lock should be enabled  
**Description:***Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 object lock not enabled. | Alarm |
| **qa tester** | **AWS** | entjedi object lock not enabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object lock not enabled. | Alarm |
| **qa tester** | **AWS** | jediar object lock not enabled. | Alarm |
| **qa tester** | **AWS** | devicedetector object lock not enabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object lock not enabled. | Alarm |
| **qa tester** | **AWS** | prytex object lock not enabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object lock not enabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object lock not enabled. | Alarm |
| **qa tester** | **AWS** | cytex object lock not enabled. | Alarm |

**Parent** **Control:** AWS Security Hub should be enabled for an AWS Account  
**Description:***AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** S3 buckets should enforce SSL  
**Description:***To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | edmsnapshots bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | testing177 bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | bstfintech bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | bstlegal bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | devicedetector bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | entjedi bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | jediar bucket policy does not enforce HTTPS. | Alarm |
| **qa tester** | **AWS** | prytex bucket policy does not enforce HTTPS. | Alarm |

**Parent** **Control:** All S3 buckets should log S3 data events in CloudTrail  
**Description:***The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | devicedetector object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object-level data events logging disabled. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress SSH access from 0.0.0.0/0  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for SSH from 0.0.0.0/0. | Ok |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** Log group encryption at rest should be enabled  
**Description:***To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Group*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | /aws/lambda/trap\_doors\_lambda not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/Color\_Picker not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/HoursOfOperation not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/color\_picker not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/color\_picker\_test not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/color\_tester not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/escapeRoomLambdaFunc not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/esportsgps not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/hello\_world\_test not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/high\_low\_game\_func not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/medical\_care not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/shippingAddress not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/stars\_test not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/testColorFunc not encrypted at rest. | Alarm |
| **qa tester** | **AWS** | /aws/lambda/test\_test not encrypted at rest. | Alarm |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** VPC flow logs should be enabled  
**Description:***The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | vpc-db2853bf flow logging disabled. | Alarm |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** Ensure that 'Secure transfer required' is set to 'Enabled'  
**Description:***Enable data encryption in transit.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b encryption in transit enabled. | Ok |

**Parent** **Control:** Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'  
**Description:***In some cases, Azure Storage sets the minimum TLS version to be version 1.0 by default. TLS 1.0 is a legacy version and has known vulnerabilities. This minimum TLS version can be configured to be later protocols such as TLS 1.2.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b minimum TLS version set to TLS1\_2. | Ok |

**Parent** **Control:** Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to ‘enabled’  
**Description:***Enabling double encryption at the hardware level on top of the default software encryption for Storage Accounts accessing Azure storage solutions.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b infrastructure encryption disabled. | Alarm |

**Parent** **Control:** Ensure Storage for Critical Data are Encrypted with Customer Managed Keys  
**Description:***Enable sensitive data encryption at rest using Customer Managed Keys rather than Microsoft Managed keys.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b not encrypted with CMK. | Alarm |

**Parent** **Control:** Ensure that VHD's are encrypted  
**Description:***VHD (Virtual Hard Disks) are stored in blob storage and are the old-style disks that were attached to Virtual Machines. The blob VHD was then leased to the VM. By default, storage accounts are not encrypted, and Microsoft Defender will then recommend that the OS disks should be encrypted. Storage accounts can be encrypted as a whole using PMK or CMK. This should be turned on for storage accounts containing VHDs.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That Microsoft Defender for Databases Is Set To 'On'  
**Description:***Turning on Microsoft Defender for Databases enables threat detection for the instances running your database software. This provides threat intelligence, anomaly detection, and behavior analytics in the Azure Microsoft Defender for Cloud. Instead of being enabled on services like Platform as a Service (PaaS), this implementation will run within your instances as Infrastructure as a Service (IaaS) on the Operating Systems hosting your databases.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Azure Defender off for Databases. | Alarm |

**Parent** **Control:** Ensure no HTTPS or SSL proxy load balancers permit SSL policies with weak cipher suites  
**Description:***Secure Sockets Layer (SSL) policies determine what port Transport Layer Security (TLS) features clients are permitted to use when connecting to load balancers.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure 'Block Project-wide SSH keys' is enabled for VM instances  
**Description:***It is recommended to use Instance specific SSH key(s) instead of using common/shared project-wide SSH key(s) to access Instances.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure VM disks for critical VMs are encrypted with Customer-Supplied Encryption Keys (CSEK)  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Compute instances have Confidential Computing enabled  
**Description:***Google Cloud encrypts data at-rest and in-transit, but customer data must be decrypted for processing. Confidential Computing is a breakthrough technology which encrypts data in-use—while it is being processed. Confidential Computing environments keep data encrypted in memory and elsewhere outside the central processing unit (CPU).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that App Engine applications enforce HTTPS connections  
**Description:***In order to maintain the highest level of security all connections to an application should be secure by default.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that the Cloud SQL database instance requires all incoming connections to use SSL  
**Description:***It is recommended to enforce all incoming connections to SQL database instance to use SSL.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure KMS encryption keys are rotated within a period of 90 days  
**Description:***Google Cloud Key Management Service stores cryptographic keys in a hierarchical structure designed for useful and elegant access control management. The format for the rotation schedule depends on the client library that is used. For the gcloud command-line tool, the next rotation time must be in ISO or RFC3339 format, and the rotation period must be in the form INTEGER[UNIT], where units can be one of seconds (s), minutes (m), hours (h) or days (d).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Key Management Service (KMS) API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/cloudkms.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "cloudkms.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that dataproc cluster is encrypted using customer-managed encryption key  
**Description:***When you use Dataproc, cluster and job data is stored on Persistent Disks (PDs) associated with the Compute Engine VMs in your cluster and in a Cloud Storage staging bucket. This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud Dataproc API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/dataproc.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/dataproc.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/cytex-85fe6"   "service": "dataproc.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager  
**Description:***Google Cloud Functions allow you to host serverless code that is executed when an event is triggered, without the requiring the management a host operating system. These functions can also store environment variables to be used by the code that may contain authentication or other information that needs to remain confidential.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

## **Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.** (NIST-PR.IP)

**NIST-PR.IP.1** A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.2** A System Development Life Cycle to manage systems is implemented

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.3** Configuration change control processes are in place

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.4** Backups of information are conducted, maintained, and tested periodically

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.5** Policy and regulations regarding the physical operating environment for organizational assets are met

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.6** Data is destroyed according to policy

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.7** Protection processes are continuously improved

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.8** Effectiveness of protection technologies is shared with appropriate parties

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.9** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.10** Response and recovery plans are tested

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.11** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.IP.12** A vulnerability management plan is developed and implemented

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** AWS Config should be enabled  
**Description:***This control checks whether AWS Config is enabled in the account for the local Region and is recording all resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | us-east-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ca-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-north-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | sa-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** DynamoDB tables should be in a backup plan  
**Description:***To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: 31b40971-8afb-440c-85fb-75653a3ffe8f  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** S3 public access should be blocked at account and bucket levels  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | cytex not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | testing177 not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | jediar not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | prytex not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket all public access blocks enabled. | Ok |

**Parent** **Control:** DynamoDB table point-in-time recovery should be enabled  
**Description:***Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game point-in-time recovery not enabled. | Alarm |

**Parent** **Control:** DynamoDB table should be protected by backup plan  
**Description:***Ensure if Amazon DynamoDB tables are protected by a backup plan. The rule is non compliant if the DynamoDB Table is not covered by a backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListProtectedResources  https response error StatusCode: 403  RequestID: 8df0f97d-d531-4e9f-aea4-af348c2be4b6  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListProtectedResources because no identity-based policy allows the backup:ListProtectedResources action (SQLSTATE HV000) | Error |

**Parent** **Control:** DynamoDB table auto scaling should be enabled  
**Description:***Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game autoscaling not enabled. | Alarm |

**Parent** **Control:** Backup plan min frequency and min retention check  
**Description:***Checks if a backup plan has a backup rule that satisfies the required frequency and retention period(35 Days). The rule is non compliant if recovery points are not created at least as often as the specified frequency or expire before the specified period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: e8bb8971-d9be-486c-91aa-79d8acbe99ea  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** VPC subnet auto assign public IP should be disabled  
**Description:***Ensure if Amazon Virtual Private Cloud (Amazon VPC) subnets are assigned a public IP address. The control is compliant if Amazon VPC does not have subnets that are assigned a public IP address. The control is non compliant if Amazon VPC has subnets that are assigned a public IP address.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | subnet-0445eb72 auto assign public IP enabled. | Alarm |
| **qa tester** | **AWS** | subnet-53cb586e auto assign public IP enabled. | Alarm |
| **qa tester** | **AWS** | subnet-35da1a6d auto assign public IP enabled. | Alarm |
| **qa tester** | **AWS** | subnet-4d8b7767 auto assign public IP enabled. | Alarm |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** Ensure Azure Keyvaults are used to store secrets  
**Description:***Encryption keys, Certificate thumbprints and Managed Identity Credentials can be coded into the APP service, this renders them visible as part of the configuration, to maintain security of these keys it is better to store in an Azure Keyvault and reference them from the Keyvault.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Security Defaults is enabled on Azure Active Directory  
**Description:***Security defaults in Azure Active Directory (Azure AD) make it easier to be secure and help protect your organization. Security defaults contain preconfigured security settings for common attacks. Microsoft is making security defaults available to everyone. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. You may turn on security defaults in the Azure portal.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Any of the ASC Default Policy Settings are Not Set to 'Disabled'  
**Description:***None of the settings offered by ASC Default policy should be set to effect Disabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Settings enabled for all the parameters. | Ok |
| **SQAE** | **Azure** | Settings enabled for all the parameters. | Ok |

**Parent** **Control:** Ensure that 'Enable key rotation reminders' is enabled for each Storage Account  
**Description:***Access Keys authenticate application access requests to data contained in Storage Accounts. A periodic rotation of these keys is recommended to ensure that potentially compromised keys cannot result in a long-term exploitable credential. The Rotation Reminder is an automatic reminder feature for a manual procedure.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That ‘Subscription Entering AAD Directory’ and ‘Subscription Leaving AAD Directory’ Is Set To ‘Permit No One’  
**Description:***Users who are set as subscription owners are able to make administrative changes to the subscriptions and move them into and out of Azure Active Directories.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Access Review is Set Up for External Users in Azure AD Privileged Identity Management  
**Description:***This recommendation extends guest access review by utilizing the Azure AD Privileged Identity Management feature provided in Azure AD Premium P2. Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data. Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources a a guest user.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Number of days before users are asked to reconfirm their authentication information' is not set to '0'  
**Description:***Ensure that the number of days before users are asked to re-confirm their authentication information is not set to 0.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Guest Users Are Reviewed on a Regular Basis  
**Description:***Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data. Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources as a guest user. Guest users in every subscription should be review on a regular basis to ensure that inactive and unneeded accounts are removed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Ensure that Storage Account Access Keys are Periodically Regenerated  
**Description:***For increased security, regenerate storage account access keys periodically.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Shared Access Signature Tokens Expire Within an Hour  
**Description:***Expire shared access signature tokens within an hour.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services  
**Description:***Automatic Key Rotation is available in Public Preview. The currently supported applications are Key Vault, Managed Disks, and Storage accounts accessing keys within Key Vault. The number of supported applications will incrementally increased.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users  
**Description:***Enable multi-factor authentication for all roles, groups, and users that have write access or permissions to Azure resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users  
**Description:***Enable multi-factor authentication for all non-privileged users.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Restore multi-factor authentication on all remembered devices' is Enabled  
**Description:***Do not allow users to remember multi-factor authentication on devices.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups  
**Description:***For designated users, they will be prompted to use their multi-factor authentication (MFA) process on login.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that A Multi-factor Authentication Policy Exists for All Users  
**Description:***For designated users, they will be prompted to use their multi-factor authentication (MFA) process on logins.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Multi-factor Authentication is Required for Risky Sign-ins  
**Description:***For designated users, they will be prompted to use their multi-factor authentication (MFA) process on login.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Multi-factor Authentication is Required for Azure Management  
**Description:***For designated users, they will be prompted to use their multi-factor authentication(MFA) process on logins.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_conditional\_access\_policy" does not exist (SQLSTATE 42P01) | Error |
| **SQAE** | **Azure** | relation "azuread\_conditional\_access\_policy" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled'  
**Description:***Do not allow users to remember multi-factor authentication on devices.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That 'Number of methods required to reset' is set to '2'  
**Description:***Ensures that two alternate forms of identification are provided before allowing a password reset.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Require Multi-Factor Authentication to register or join devices with Azure AD' is set to 'Yes'  
**Description:***Joining or registering devices to the active directory should require Multi-factor authentication.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Trusted Locations Are Defined  
**Description:***Azure Active Directory Conditional Access allows an organization to configure Named locations and configure whether those locations are trusted or untrusted. These settings provide organizations the means to specify Geographical locations for use in conditional access policies, or define actual IP addresses and IP ranges and whether or not those IP addresses and/or ranges are trusted by the organization.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that an exclusionary Geographic Access Policy is considered  
**Description:***Conditional Access Policies can be used to block access from geographic locations that are deemed out-of-scope for your organization or application. The scope and variables for this policy should be carefully examined and defined.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization  
**Description:***Microsoft Azure creates a default bad password policy that is already applied to Azure administrative and normal user accounts. This is not applied to user accounts that are synced from an on-premise Active Directory unless Azure AD Connect is used and you enable EnforceCloudPasswordPolicyForPasswordSyncedUsers. Please see the list in default values on the specifics of this policy.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Notify users on password resets?' is set to 'Yes'  
**Description:***Ensure that users are notified on their primary and secondary emails on password resets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes'  
**Description:***Ensure that all administrators are notified if any other administrator resets their password.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That ‘Users Can Consent to Apps Accessing Company Data on Their Behalf’ Is Set To ‘Allow for Verified Publishers’  
**Description:***Allow users to provide consent for selected permissions when a request is coming from a verified publisher.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No'  
**Description:***Require administrators to provide consent for the apps before use.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That ‘Users Can Register Applications’ Is Set to ‘No’  
**Description:***Require administrators or appropriately delegated users to register third-party applications.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_authorization\_policy" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'  
**Description:***Limit guest user permissions.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On'  
**Description:***Enable automatic provisioning of the monitoring agent to collect security data.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Automatic provisioning of monitoring agent is off. | Alarm |

**Parent** **Control:** Ensure that Auto provisioning of 'Vulnerability assessment for machines' is Set to 'On'  
**Description:***Enable automatic provisioning of vulnerability assessment for machines on both Azure and hybrid (Arc enabled) machines.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On'  
**Description:***Enable automatic provisioning of the Microsoft Defender for Containers components.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Soft Delete is Enabled for Azure Containers and Blob Storage  
**Description:***The Azure Storage blobs contain data like ePHI or Financial, which can be secret or personal. Data that is erroneously modified or deleted by an application or other storage account user will cause data loss or unavailability. It is recommended that both Azure Containers with attached Blob Storage and standalone containers with Blob Storage be made recoverable by enabling the soft delete configuration. This is to save and recover data when blobs or blob snapshots are deleted.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b blobs soft delete disabled. | Alarm |

**Parent** **Control:** Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off'  
**Description:***It is recommended to set external scripts enabled database flag for Cloud SQL SQL Server instance to off.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured  
**Description:***It is recommended that, user options database flag for Cloud SQL SQL Server instance should not be configured.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that the default network does not exist in a project  
**Description:***To prevent use of default network, a project should not have a default network.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure legacy networks do not exist for a project  
**Description:***In order to prevent use of legacy networks, a project should not have a legacy network configured.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that DNSSEC is enabled for Cloud DNS  
**Description:***Cloud Domain Name System (DNS) is a fast, reliable and cost-effective domain name system that powers millions of domains on the internet. 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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud DNS API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/dns.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/dns.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/cytex-85fe6"   "service": "dns.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that RSASHA1 is not used for the key-signing key in Cloud DNS DNSSEC  
**Description:***DNSSEC algorithm numbers in this registry may be used in CERT RRs. Zone signing (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms. The algorithm used for key signing should be a recommended one and it should be strong.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud DNS API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/dns.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/dns.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/cytex-85fe6"   "service": "dns.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that RSASHA1 is not used for the zone-signing key in Cloud DNS DNSSEC  
**Description:***DNSSEC algorithm numbers in this registry may be used in CERT RRs. Zone signing (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms. The algorithm used for key signing should be a recommended one and it should be strong.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud DNS API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/dns.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/dns.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/cytex-85fe6"   "service": "dns.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Cloud SQL database instances are configured with automated backups  
**Description:***It is recommended to have all SQL database instances set to enable automated backups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

## **Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.** (NIST-PR.MA)

**NIST-PR.MA.1** Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.MA.2** Remote maintenance of organizational assets are approved, logged, and performed in a manner that prevents unauthorized access

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access  
**Description:***Some Azure services that interact with storage accounts operate from networks that can't be granted access through network rules. To help this type of service work as intended, allow the set of trusted Azure services to bypass the network rules. These services will then use strong authentication to access the storage account. If the Allow trusted Azure services exception is enabled, the following services are granted access to the storage account: Azure Backup, Azure Site Recovery, Azure DevTest Labs, Azure Event Grid, Azure Event Hubs, Azure Networking, Azure Monitor, and Azure SQL Data Warehouse (when registered in the subscription).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b trusted Microsoft services enabled. | Ok |

## **Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.** (NIST-PR.PT)

**NIST-PR.PT.1** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.PT.2** Removable media is protected and its use restricted according to policy

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.PT.3** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.PT.4** Communications and control networks are protected

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-PR.PT.5** Systems operate in pre.defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations)

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** IAM policy should not have statements with admin access  
**Description:***AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing 'Effect': 'Allow' with 'Action': '\*' over 'Resource': '\*'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | AWSLambdaEdgeExecutionRole-adc0e8e5-65d9-40a5-aaff-752d94f98e81 contains 0 statements that allow action "\*" on resource "\*". | Ok |
| **qa tester** | **AWS** | cytexaudit\_sploit contains 0 statements that allow action "\*" on resource "\*". | Ok |

**Parent** **Control:** VPC flow logs should be enabled  
**Description:***The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | vpc-db2853bf flow logging disabled. | Alarm |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

**Parent** **Control:** S3 public access should be blocked at account level  
**Description:***Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Account level public access blocks not enabled for: block\_public\_acls  block\_public\_policy  ignore\_public\_acls  restrict\_public\_buckets. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress SSH access from 0.0.0.0/0  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for SSH from 0.0.0.0/0. | Ok |

**Parent** **Control:** API Gateway stage logging should be enabled  
**Description:***API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | beta logging not enabled. | Alarm |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** S3 buckets should prohibit public read access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 publicly readable. | Alarm |
| **qa tester** | **AWS** | prytex not publicly readable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly readable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly readable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly readable. | Ok |
| **qa tester** | **AWS** | cytex not publicly readable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly readable. | Ok |
| **qa tester** | **AWS** | jediar not publicly readable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly readable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly readable. | Ok |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** Lambda functions should restrict public access  
**Description:***Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test does not allow public access. | Ok |
| **qa tester** | **AWS** | trap\_doors\_lambda does not allow public access. | Ok |
| **qa tester** | **AWS** | escapeRoomLambdaFunc does not allow public access. | Ok |
| **qa tester** | **AWS** | esportsgps does not allow public access. | Ok |
| **qa tester** | **AWS** | medical\_care does not allow public access. | Ok |

**Parent** **Control:** VPC security groups should restrict ingress TCP and UDP access from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a does not allow ingress to TCP or UDP ports from 0.0.0.0/0. | Ok |

**Parent** **Control:** IAM root user should not have access keys  
**Description:***Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No root user access keys exist. | Ok |

**Parent** **Control:** IAM user should not have any inline or attached policies  
**Description:***This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | cytex has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | cytexaudit has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | jediar has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | s3readonly has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | taimur has 0 inline and 1 directly attached policies. | Alarm |
| **qa tester** | **AWS** | testcytex has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | farrukh has 0 inline and 0 directly attached policies. | Ok |
| **qa tester** | **AWS** | prytex has 0 inline and 0 directly attached policies. | Ok |

**Parent** **Control:** S3 buckets should prohibit public write access  
**Description:***Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not publicly writable. | Ok |
| **qa tester** | **AWS** | bstfintech not publicly writable. | Ok |
| **qa tester** | **AWS** | prytex not publicly writable. | Ok |
| **qa tester** | **AWS** | entjedi not publicly writable. | Ok |
| **qa tester** | **AWS** | jediar not publicly writable. | Ok |
| **qa tester** | **AWS** | cytex not publicly writable. | Ok |
| **qa tester** | **AWS** | bstlegal not publicly writable. | Ok |
| **qa tester** | **AWS** | devicedetector not publicly writable. | Ok |
| **qa tester** | **AWS** | edmsnapshots not publicly writable. | Ok |
| **qa tester** | **AWS** | usdztestingbucket not publicly writable. | Ok |

**Parent** **Control:** VPC security groups should restrict ingress access on ports 20, 21, 22, 3306, 3389, 4333 from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for ports 20  21  22  3306  3389  4333 from 0.0.0.0/0. | Ok |

**Parent** **Control:** Lambda functions should be in a VPC  
**Description:***Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test is not in VPC. | Alarm |
| **qa tester** | **AWS** | trap\_doors\_lambda is not in VPC. | Alarm |
| **qa tester** | **AWS** | escapeRoomLambdaFunc is not in VPC. | Alarm |
| **qa tester** | **AWS** | esportsgps is not in VPC. | Alarm |
| **qa tester** | **AWS** | medical\_care is not in VPC. | Alarm |

**Parent** **Control:** Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off'  
**Description:***It is recommended to set external scripts enabled database flag for Cloud SQL SQL Server instance to off.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that sinks are configured for all log entries  
**Description:***It is recommended to create a sink that will export copies of all the log entries. This can help aggregate logs from multiple projects and export them to a Security Information and Event Management (SIEM).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Sinks not configured for all log entries. | Alarm |

**Parent** **Control:** Ensure log metric filter and alerts exist for project ownership assignments/changes  
**Description:***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. Members (users/Service-Accounts) with a role assignment to primitive role roles/Owner are project owners.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist exist for project ownership assignments/changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for Audit Configuration changes  
**Description:***Cloud audit logging records information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by GCP services. Cloud audit logging provides a history of GCP API calls for an account, including API calls made via the console, SDKs, command-line tools, and other GCP services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for audit configuration changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for Custom Role changes  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for custom role changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for VPC Network Firewall rule changes  
**Description:***It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) Network Firewall rule changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist network for firewall rule changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for VPC network route changes  
**Description:***It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network route changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for network route changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for VPC network changes  
**Description:***It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for network changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for Cloud Storage IAM permission changes  
**Description:***It is recommended that a metric filter and alarm be established for Cloud Storage Bucket IAM changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for Storage IAM permission changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for SQL instance configuration changes  
**Description:***It is recommended that a metric filter and alarm be established for SQL instance configuration changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for SQL instance configuration changes. | Alarm |

**Parent** **Control:** Ensure that Cloud DNS logging is enabled for all VPC networks  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure 'Access Transparency' is 'Enabled'  
**Description:***GCP Access Transparency provides audit logs for all actions that Google personnel take in your Google Cloud resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that VPC Flow Logs is enabled for every subnet in a VPC Network  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

# Risk Management

## **Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.** (NIST-DE.AE)

**NIST-DE.AE.1** A baseline of network operations and expected data flows for users and systems is established and managed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.AE.2** Detected events are analyzed to understand attack targets and methods

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.AE.3** Event data are collected and correlated from multiple sources and sensors

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.AE.4** Impact of events is determined

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.AE.5** Incident alert thresholds are established

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** API Gateway stage logging should be enabled  
**Description:***API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | beta logging not enabled. | Alarm |
| **qa tester** | **AWS** | beta logging not enabled. | Alarm |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** Lambda functions concurrent execution limit configured  
**Description:***Checks whether the AWS Lambda function is configured with function-level concurrent execution limit. The control is non compliant if the Lambda function is not configured with function-level concurrent execution limit.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | table 'aws\_lambda\_function' column 'reserved\_concurrent\_executions' requires hydrate data from getAwsLambdaFunction  which failed with error operation error Lambda: GetFunction  https response error StatusCode: 403  RequestID: 9c92aa95-c785-44ae-9179-bbe8e58ff199  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: lambda:GetFunction on resource: arn:aws:lambda:us-east-1:986601184113:function:esportsgps because no identity-based policy allows the lambda:GetFunction action.  (SQLSTATE HV000) | Error |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** VPC default security group should not allow inbound and outbound traffic  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Default security group sg-7344060a has inbound and outbound rules. | Alarm |

**Parent** **Control:** VPC flow logs should be enabled  
**Description:***The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | vpc-db2853bf flow logging disabled. | Alarm |
| **qa tester** | **AWS** | vpc-db2853bf flow logging disabled. | Alarm |

**Parent** **Control:** VPC security groups should restrict ingress access on ports 20, 21, 22, 3306, 3389, 4333 from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for ports 20  21  22  3306  3389  4333 from 0.0.0.0/0. | Ok |

**Parent** **Control:** VPC security groups should restrict ingress SSH access from 0.0.0.0/0  
**Description:***Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a ingress restricted for SSH from 0.0.0.0/0. | Ok |

**Parent** **Control:** VPC security groups should restrict ingress TCP and UDP access from 0.0.0.0/0  
**Description:***Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | sg-7344060a does not allow ingress to TCP or UDP ports from 0.0.0.0/0. | Ok |

**Parent** **Control:** GuardDuty should be enabled  
**Description:***Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** AWS Security Hub should be enabled for an AWS Account  
**Description:***AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** All S3 buckets should log S3 data events in CloudTrail  
**Description:***The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | devicedetector object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object-level data events logging disabled. | Alarm |

**Parent** **Control:** CloudWatch alarm should have an action configured  
**Description:***Checks if CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT\_DATA, or OK state. Optionally checks if any actions match a named ARN. The rule is non compliant if there is no action specified for the alarm or optional parameter.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game-WriteCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |
| **qa tester** | **AWS** | High-Low-Game-ReadCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |

**Parent** **Control:** Lambda functions should be configured with a dead-letter queue  
**Description:***Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | stars\_test configured with dead-letter queue. | Alarm |
| **qa tester** | **AWS** | esportsgps configured with dead-letter queue. | Alarm |
| **qa tester** | **AWS** | medical\_care configured with dead-letter queue. | Alarm |
| **qa tester** | **AWS** | trap\_doors\_lambda configured with dead-letter queue. | Alarm |
| **qa tester** | **AWS** | escapeRoomLambdaFunc configured with dead-letter queue. | Alarm |
| **qa tester** | **AWS** | stars\_test configured with dead-letter queue. | Alarm |
| **qa tester** | **AWS** | trap\_doors\_lambda configured with dead-letter queue. | Alarm |
| **qa tester** | **AWS** | escapeRoomLambdaFunc configured with dead-letter queue. | Alarm |
| **qa tester** | **AWS** | esportsgps configured with dead-letter queue. | Alarm |
| **qa tester** | **AWS** | medical\_care configured with dead-letter queue. | Alarm |

**Parent** **Control:** Ensure That 'Notify about alerts with the following severity' is Set to 'High'  
**Description:***Enables emailing security alerts to the subscription owner or other designated security contact.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | "Notify about alerts with the following severity" not set to High. | Alarm |

**Parent** **Control:** Ensure that Storage Account Access Keys are Periodically Regenerated  
**Description:***For increased security, regenerate storage account access keys periodically.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Guest Users Are Reviewed on a Regular Basis  
**Description:***Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data. Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources as a guest user. Guest users in every subscription should be review on a regular basis to ensure that inactive and unneeded accounts are removed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' request  
**Description:***The Storage Queue service stores messages that may be read by any client who has access to the storage account. A queue can contain an unlimited number of messages, each of which can be up to 64KB in size using version 2011-08-18 or newer. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the queues. Storage Logging log entries contain the following information about individual requests: Timing information such as start time, end-to-end latency, and server latency, authentication details, concurrency information, and the sizes of the request and response messages.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | table 'azure\_storage\_account' column 'queue\_logging\_retention\_enabled' requires hydrate data from getAzureStorageAccountQueueProperties  which failed with error storage.AccountsClient#ListKeys: Failure responding to request: StatusCode=403 -- Original Error: autorest/azure: Service returned an error. Status=403 Code="AuthorizationFailed" Message="The client '3048e5a6-10f9-4dac-892e-1ff1732f65e2' with object id '3048e5a6-10f9-4dac-892e-1ff1732f65e2' does not have authorization to perform action 'Microsoft.Storage/storageAccounts/listKeys/action' over scope '/subscriptions/195d31b2-d396-4dce-a6b3-d7275f741c2b/resourceGroups/cloud-shell-storage-eastus/providers/Microsoft.Storage/storageAccounts/cs210032000de891a1b' or the scope is invalid. If access was recently granted  please refresh your credentials.".  (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that Shared Access Signature Tokens Expire Within an Hour  
**Description:***Expire shared access signature tokens within an hour.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Enable key rotation reminders' is enabled for each Storage Account  
**Description:***Access Keys authenticate application access requests to data contained in Storage Accounts. A periodic rotation of these keys is recommended to ensure that potentially compromised keys cannot result in a long-term exploitable credential. The Rotation Reminder is an automatic reminder feature for a manual procedure.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests  
**Description:***The Storage Blob service provides scalable, cost-efficient object storage in the cloud. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the blobs. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | storage.AccountsClient#ListKeys: Failure responding to request: StatusCode=403 -- Original Error: autorest/azure: Service returned an error. Status=403 Code="AuthorizationFailed" Message="The client '3048e5a6-10f9-4dac-892e-1ff1732f65e2' with object id '3048e5a6-10f9-4dac-892e-1ff1732f65e2' does not have authorization to perform action 'Microsoft.Storage/storageAccounts/listKeys/action' over scope '/subscriptions/195d31b2-d396-4dce-a6b3-d7275f741c2b/resourceGroups/cloud-shell-storage-eastus/providers/Microsoft.Storage/storageAccounts/cs210032000de891a1b' or the scope is invalid. If access was recently granted  please refresh your credentials." (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests  
**Description:***Azure Table storage is a service that stores structured NoSQL data in the cloud, providing a key/attribute store with a schema-less design. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the tables. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create Policy Assignment  
**Description:***Create an activity log alert for the Create Policy Assignment event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for create policy assignment event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete Policy Assignment  
**Description:***Create an activity log alert for the Delete Policy Assignment event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for delete policy assignment event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create or Update Network Security Group  
**Description:***Create an Activity Log Alert for the Create or Update Network Security Group event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for create or update Network Security Group event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete Network Security Group  
**Description:***Create an activity log alert for the Delete Network Security Group event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for delete Network Security Group event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create or Update Security Solution  
**Description:***Create an activity log alert for the Create or Update Security Solution event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for create or update Security Solution event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete Security Solution  
**Description:***Create an activity log alert for the Delete Security Solution event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for delete Security Solution event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule  
**Description:***Create an activity log alert for the Create or Update SQL Server Firewall Rule event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity Log Alert does not exists for Create or Update SQL Server Firewall Rule. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule  
**Description:***Create an activity log alert for the 'Delete SQL Server Firewall Rule.'*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity Log Alert does not exists for Delete SQL Server Firewall Rule. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create or Update Public IP Address rule  
**Description:***Create an activity log alert for the Create or Update Public IP Addresses rule.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity Log Alert does not exists for Create or Update Public IP Address rule. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete Public IP Address rule  
**Description:***Create an activity log alert for the Delete Public IP Address rule.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity Log Alert does not exists for Delete Public IP Address rule. | Alarm |

**Parent** **Control:** Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it  
**Description:***Resource Logs capture activity to the data access plane while the Activity log is a subscription-level log for the control plane. Resource-level diagnostic logs provide insight into operations that were performed within that resource itself; for example, reading or updating a secret from a Key Vault.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that logging for Azure AppService 'AppServiceHTTPLogs' is enabled.  
**Description:***Enable AppServiceHTTPLogs diagnostic log category for Azure App Service instances to ensure all http requests are captured and centrally logged.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that sinks are configured for all log entries  
**Description:***It is recommended to create a sink that will export copies of all the log entries. This can help aggregate logs from multiple projects and export them to a Security Information and Event Management (SIEM).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Sinks not configured for all log entries. | Alarm |

**Parent** **Control:** Ensure log metric filter and alerts exist for project ownership assignments/changes  
**Description:***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. Members (users/Service-Accounts) with a role assignment to primitive role roles/Owner are project owners.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist exist for project ownership assignments/changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for Audit Configuration changes  
**Description:***Cloud audit logging records information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by GCP services. Cloud audit logging provides a history of GCP API calls for an account, including API calls made via the console, SDKs, command-line tools, and other GCP services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for audit configuration changes. | Alarm |
| **QA tester** | **Gcp** | Log metric and alert do not exist for audit configuration changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for Custom Role changes  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for custom role changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for VPC Network Firewall rule changes  
**Description:***It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) Network Firewall rule changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist network for firewall rule changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for VPC network route changes  
**Description:***It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network route changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for network route changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for VPC network changes  
**Description:***It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for network changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for Cloud Storage IAM permission changes  
**Description:***It is recommended that a metric filter and alarm be established for Cloud Storage Bucket IAM changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for Storage IAM permission changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for SQL instance configuration changes  
**Description:***It is recommended that a metric filter and alarm be established for SQL instance configuration changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for SQL instance configuration changes. | Alarm |

**Parent** **Control:** Ensure that Cloud DNS logging is enabled for all VPC networks  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure 'Access Transparency' is 'Enabled'  
**Description:***GCP Access Transparency provides audit logs for all actions that Google personnel take in your Google Cloud resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that VPC Flow Logs is enabled for every subnet in a VPC Network  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that a MySQL database instance does not allow anyone to connect with administrative privileges  
**Description:***It is recommended to set a password for the administrative user (root by default) to prevent unauthorized access to the SQL database instances. This recommendation is applicable only for MySQL Instances. PostgreSQL does not offer any setting for No Password from the cloud console.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that the 'log\_connections' database flag for Cloud SQL PostgreSQL instance is set to 'on'  
**Description:***Enabling the log\_connections setting causes each attempted connection to the server to be logged, along with successful completion of client authentication. This parameter cannot be changed after the session starts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that the 'log\_disconnections' database flag for Cloud SQL PostgreSQL instance is set to 'on'  
**Description:***Enabling the log\_disconnections setting logs the end of each session, including the session duration.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure 'log\_statement' database flag for Cloud SQL PostgreSQL instance is set appropriately  
**Description:***The value of log\_statement flag determined the SQL statements that are logged. Valid values are: 'none', 'ddl', 'mod', and 'all'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure 'log\_hostname' database flag for Cloud SQL PostgreSQL instance is set appropriately  
**Description:***PostgreSQL logs only the IP address of the connecting hosts. The log\_hostname flag controls the logging of hostnames in addition to the IP addresses logged. The performance hit is dependent on the configuration of the environment and the host name resolution setup. This parameter can only be set in the postgresql.conf file or on the server command line.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that the 'log\_min\_messages' database flag for Cloud SQL PostgreSQL instance is set appropriately  
**Description:***The log\_min\_messages flag defines the minimum message severity level that is considered as an error statement. Messages for error statements are logged with the SQL statement. Valid values include DEBUG5, DEBUG4, DEBUG3, DEBUG2, DEBUG1, INFO, NOTICE, WARNING, ERROR, LOG, FATAL, and PANIC. Each severity level includes the subsequent levels mentioned above.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure 'log\_min\_error\_statement' database flag for Cloud SQL PostgreSQL instance is set to 'Error' or stricter  
**Description:***The log\_min\_error\_statement flag defines the minimum message severity level that are considered as an error statement. Messages for error statements are logged with the SQL statement. Valid values include DEBUG5, DEBUG4, DEBUG3, DEBUG2, DEBUG1, INFO, NOTICE, WARNING, ERROR, LOG, FATAL, and PANIC. Each severity level includes the subsequent levels mentioned above. Ensure a value of ERROR or stricter is set.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that the 'log\_min\_duration\_statement' database flag for Cloud SQL PostgreSQL instance is set to '-1' (disabled)  
**Description:***The log\_min\_duration\_statement flag defines the minimum amount of execution time of a statement in milliseconds where the total duration of the statement is logged. Ensure that log\_min\_duration\_statement is disabled, i.e., a value of -1 is set.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure That 'cloudsql.enable\_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging  
**Description:***Ensure cloudsql.enable\_pgaudit database flag for Cloud SQL PostgreSQL instance is set to on to allow for centralized logging.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

## **Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.** (NIST-DE.CM)

**NIST-DE.CM.1** The network is monitored to detect potential cybersecurity events

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.CM.2** The physical environment is monitored to detect potential cybersecurity events

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.CM.3** Personnel activity is monitored to detect potential cybersecurity events

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.CM.4** Malicious code is detected

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.CM.5** Unauthorized mobile code is detected

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.CM.6** External service provider activity is monitored to detect potential cybersecurity events

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.CM.7** Monitoring for unauthorized personnel, connections, devices, and software is performed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.CM.8** Vulnerability scans are performed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** API Gateway stage logging should be enabled  
**Description:***API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | beta logging not enabled. | Alarm |
| **qa tester** | **AWS** | beta logging not enabled. | Alarm |

**Parent** **Control:** At least one multi-region AWS CloudTrail should be present in an account  
**Description:***AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED is enabled.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |
| **qa tester** | **AWS** | 986601184113 does not have multi-region trail(s). | Alarm |

**Parent** **Control:** All S3 buckets should log S3 data events in CloudTrail  
**Description:***The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | devicedetector object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket object-level data events logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots object-level data events logging disabled. | Alarm |

**Parent** **Control:** GuardDuty should be enabled  
**Description:***Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** S3 bucket logging should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |
| **qa tester** | **AWS** | entjedi logging disabled. | Alarm |
| **qa tester** | **AWS** | cytex logging disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket logging disabled. | Alarm |
| **qa tester** | **AWS** | testing177 logging disabled. | Alarm |
| **qa tester** | **AWS** | jediar logging disabled. | Alarm |
| **qa tester** | **AWS** | prytex logging disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots logging disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech logging disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector logging disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal logging disabled. | Alarm |

**Parent** **Control:** AWS Security Hub should be enabled for an AWS Account  
**Description:***AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** VPC flow logs should be enabled  
**Description:***The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | vpc-db2853bf flow logging disabled. | Alarm |
| **qa tester** | **AWS** | vpc-db2853bf flow logging disabled. | Alarm |

**Parent** **Control:** CloudWatch alarm should have an action configured  
**Description:***Checks if CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT\_DATA, or OK state. Optionally checks if any actions match a named ARN. The rule is non compliant if there is no action specified for the alarm or optional parameter.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game-WriteCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |
| **qa tester** | **AWS** | High-Low-Game-ReadCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |
| **qa tester** | **AWS** | High-Low-Game-WriteCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |
| **qa tester** | **AWS** | High-Low-Game-ReadCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |

**Parent** **Control:** AWS Config should be enabled  
**Description:***This control checks whether AWS Config is enabled in the account for the local Region and is recording all resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | us-east-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ca-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-central-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-north-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | eu-west-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-3 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-northeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | sa-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-southeast-2 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | us-east-1 IncludeGlobalResourceTypes disabled  AllSupported disabled  Recording disabled and LastStatus is not SUCCESS. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** Ensure a log metric filter and alarm exist for S3 bucket policy changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to S3 bucket policies. Monitoring these changes might reduce time to detect and correct permissive policies on sensitive S3 buckets.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for S3 bucket policy changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for CloudTrail configuration changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to CloudTrail configuration settings. Monitoring these changes helps ensure sustained visibility to activities in the account.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for CloudTrail configuration changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Config configuration changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes to AWS Config configuration settings. Monitoring these changes helps ensure sustained visibility of configuration items in the account*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for AWS Config configuration changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Management Console authentication failures  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for failed console authentication attempts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for console authentication failures. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for AWS Management Console sign-in without MFA  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm console logins that aren't protected by MFA.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for console sign-in without MFA. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer managed keys  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for customer managed keys that have changed state to disabled or scheduled deletion. Data encrypted with disabled or deleted keys is no longer accessible.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for disabling/deletion of CMKs. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for IAM policy changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Security Hub recommends that you create a metric filter and alarm for changes made to IAM policies. Monitoring these changes helps ensure that authentication and authorization controls remain intact.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for IAM policy changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)  
**Description:***You can do real-time monitoring of API calls 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 in a VPC. Security Hub recommends that you create a metric filter and alarm for changes to NACLs. Monitoring these changes helps ensure that AWS resources and services aren't unintentionally exposed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for changes to NACLs. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for changes to network gateways  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Network gateways are required to send and receive traffic to a destination outside a VPC. Security Hub recommends that you create a metric filter and alarm for changes to network gateways.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for changes to network gateways. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for usage of 'root' account  
**Description:***You can do real-time monitoring of API calls directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms.Security Hub recommends that you create a metric filter and alarm for root login attempts. Monitoring for root account logins provides visibility into the use of a fully privileged account and an opportunity to reduce the use of it.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for usage of "root" account. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for route table changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Routing tables route network traffic between subnets and to network gateways. Security Hub recommends that you create a metric filter and alarm for changes to route tables. Monitoring these changes helps ensure that all VPC traffic flows through an expected path.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for route table changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for security group changes  
**Description:***You can do real-time monitoring of API calls 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 in a VPC. Security Hub recommends that you create a metric filter and alarm for changes to security groups. Monitoring these changes helps ensure that resources and services aren't unintentionally exposed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for security group changes. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for unauthorized API calls  
**Description:***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 recommended that a metric filter and alarm be established for unauthorized API calls.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for unauthorized API calls. | Alarm |

**Parent** **Control:** Ensure a log metric filter and alarm exist for VPC changes  
**Description:***You can do real-time monitoring of API calls by directing CloudTrail logs to CloudWatch Logs and establishing corresponding metric filters and alarms. You can have more than one VPC in an account, and you can create a peer connection between two VPCs, enabling network traffic to route between VPCs. Security Hub recommends that you create a metric filter and alarm for changes to VPCs.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No log metric filter and alarm exist for VPC changes. | Alarm |

**Parent** **Control:** Ensure That ‘Users Can Consent to Apps Accessing Company Data on Their Behalf’ Is Set To ‘Allow for Verified Publishers’  
**Description:***Allow users to provide consent for selected permissions when a request is coming from a verified publisher.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No'  
**Description:***Require administrators to provide consent for the apps before use.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that 'Users can add gallery apps to My Apps' is set to 'No'  
**Description:***Require administrators to provide consent for the apps before use.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure That ‘Users Can Register Applications’ Is Set to ‘No’  
**Description:***Require administrators or appropriately delegated users to register third-party applications.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_authorization\_policy" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Ensure That Microsoft Defender for Databases Is Set To 'On'  
**Description:***Turning on Microsoft Defender for Databases enables threat detection for the instances running your database software. This provides threat intelligence, anomaly detection, and behavior analytics in the Azure Microsoft Defender for Cloud. Instead of being enabled on services like Platform as a Service (PaaS), this implementation will run within your instances as Infrastructure as a Service (IaaS) on the Operating Systems hosting your databases.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Azure Defender off for Databases. | Alarm |

**Parent** **Control:** Ensure That Microsoft Defender for IoT Is Set To 'On'  
**Description:***Microsoft Defender for IoT acts as a central security hub for IoT devices within your organization.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On'  
**Description:***Enable automatic provisioning of the monitoring agent to collect security data.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Automatic provisioning of monitoring agent is off. | Alarm |

**Parent** **Control:** Ensure that Auto provisioning of 'Vulnerability assessment for machines' is Set to 'On'  
**Description:***Enable automatic provisioning of vulnerability assessment for machines on both Azure and hybrid (Arc enabled) machines.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On'  
**Description:***Enable automatic provisioning of the Microsoft Defender for Containers components.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Storage Account Access Keys are Periodically Regenerated  
**Description:***For increased security, regenerate storage account access keys periodically.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure Guest Users Are Reviewed on a Regular Basis  
**Description:***Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data. Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources as a guest user. Guest users in every subscription should be review on a regular basis to ensure that inactive and unneeded accounts are removed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | relation "azuread\_user" does not exist (SQLSTATE 42P01) | Error |

**Parent** **Control:** Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' request  
**Description:***The Storage Queue service stores messages that may be read by any client who has access to the storage account. A queue can contain an unlimited number of messages, each of which can be up to 64KB in size using version 2011-08-18 or newer. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the queues. Storage Logging log entries contain the following information about individual requests: Timing information such as start time, end-to-end latency, and server latency, authentication details, concurrency information, and the sizes of the request and response messages.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | table 'azure\_storage\_account' column 'queue\_logging\_retention\_enabled' requires hydrate data from getAzureStorageAccountQueueProperties  which failed with error storage.AccountsClient#ListKeys: Failure responding to request: StatusCode=403 -- Original Error: autorest/azure: Service returned an error. Status=403 Code="AuthorizationFailed" Message="The client '3048e5a6-10f9-4dac-892e-1ff1732f65e2' with object id '3048e5a6-10f9-4dac-892e-1ff1732f65e2' does not have authorization to perform action 'Microsoft.Storage/storageAccounts/listKeys/action' over scope '/subscriptions/195d31b2-d396-4dce-a6b3-d7275f741c2b/resourceGroups/cloud-shell-storage-eastus/providers/Microsoft.Storage/storageAccounts/cs210032000de891a1b' or the scope is invalid. If access was recently granted  please refresh your credentials.".  (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests  
**Description:***The Storage Blob service provides scalable, cost-efficient object storage in the cloud. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the blobs. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | storage.AccountsClient#ListKeys: Failure responding to request: StatusCode=403 -- Original Error: autorest/azure: Service returned an error. Status=403 Code="AuthorizationFailed" Message="The client '3048e5a6-10f9-4dac-892e-1ff1732f65e2' with object id '3048e5a6-10f9-4dac-892e-1ff1732f65e2' does not have authorization to perform action 'Microsoft.Storage/storageAccounts/listKeys/action' over scope '/subscriptions/195d31b2-d396-4dce-a6b3-d7275f741c2b/resourceGroups/cloud-shell-storage-eastus/providers/Microsoft.Storage/storageAccounts/cs210032000de891a1b' or the scope is invalid. If access was recently granted  please refresh your credentials." (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests  
**Description:***Azure Table storage is a service that stores structured NoSQL data in the cloud, providing a key/attribute store with a schema-less design. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the tables. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Network Security Group Flow logs are captured and sent to Log Analytics  
**Description:***Ensure that network flow logs are captured and fed into a central log analytics workspace.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create Policy Assignment  
**Description:***Create an activity log alert for the Create Policy Assignment event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for create policy assignment event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete Policy Assignment  
**Description:***Create an activity log alert for the Delete Policy Assignment event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for delete policy assignment event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create or Update Network Security Group  
**Description:***Create an Activity Log Alert for the Create or Update Network Security Group event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for create or update Network Security Group event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete Network Security Group  
**Description:***Create an activity log alert for the Delete Network Security Group event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for delete Network Security Group event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create or Update Security Solution  
**Description:***Create an activity log alert for the Create or Update Security Solution event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for create or update Security Solution event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete Security Solution  
**Description:***Create an activity log alert for the Delete Security Solution event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity log alert does not exists for delete Security Solution event. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule  
**Description:***Create an activity log alert for the Create or Update SQL Server Firewall Rule event.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity Log Alert does not exists for Create or Update SQL Server Firewall Rule. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule  
**Description:***Create an activity log alert for the 'Delete SQL Server Firewall Rule.'*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity Log Alert does not exists for Delete SQL Server Firewall Rule. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Create or Update Public IP Address rule  
**Description:***Create an activity log alert for the Create or Update Public IP Addresses rule.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity Log Alert does not exists for Create or Update Public IP Address rule. | Alarm |

**Parent** **Control:** Ensure that Activity Log Alert exists for Delete Public IP Address rule  
**Description:***Create an activity log alert for the Delete Public IP Address rule.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Activity Log Alert does not exists for Delete Public IP Address rule. | Alarm |

**Parent** **Control:** Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it  
**Description:***Resource Logs capture activity to the data access plane while the Activity log is a subscription-level log for the control plane. Resource-level diagnostic logs provide insight into operations that were performed within that resource itself; for example, reading or updating a secret from a Key Vault.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that the endpoint protection for all Virtual Machines is installed  
**Description:***Install endpoint protection for all virtual machines.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Manual verification required. | Manual |

**Parent** **Control:** Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access  
**Description:***Some Azure services that interact with storage accounts operate from networks that can't be granted access through network rules. To help this type of service work as intended, allow the set of trusted Azure services to bypass the network rules. These services will then use strong authentication to access the storage account. If the Allow trusted Azure services exception is enabled, the following services are granted access to the storage account: Azure Backup, Azure Site Recovery, Azure DevTest Labs, Azure Event Grid, Azure Event Hubs, Azure Networking, Azure Monitor, and Azure SQL Data Warehouse (when registered in the subscription).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | cs210032000de891a1b trusted Microsoft services enabled. | Ok |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for Audit Configuration changes  
**Description:***Cloud audit logging records information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by GCP services. Cloud audit logging provides a history of GCP API calls for an account, including API calls made via the console, SDKs, command-line tools, and other GCP services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for audit configuration changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for Custom Role changes  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for custom role changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for VPC Network Firewall rule changes  
**Description:***It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) Network Firewall rule changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist network for firewall rule changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for VPC network route changes  
**Description:***It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network route changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for network route changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for VPC network changes  
**Description:***It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for network changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for Cloud Storage IAM permission changes  
**Description:***It is recommended that a metric filter and alarm be established for Cloud Storage Bucket IAM changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for Storage IAM permission changes. | Alarm |

**Parent** **Control:** Ensure that the log metric filter and alerts exist for SQL instance configuration changes  
**Description:***It is recommended that a metric filter and alarm be established for SQL instance configuration changes.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Log metric and alert do not exist for SQL instance configuration changes. | Alarm |

**Parent** **Control:** Ensure 'Access Transparency' is 'Enabled'  
**Description:***GCP Access Transparency provides audit logs for all actions that Google personnel take in your Google Cloud resources.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that a MySQL database instance does not allow anyone to connect with administrative privileges  
**Description:***It is recommended to set a password for the administrative user (root by default) to prevent unauthorized access to the SQL database instances. This recommendation is applicable only for MySQL Instances. PostgreSQL does not offer any setting for No Password from the cloud console.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure that the 'log\_connections' database flag for Cloud SQL PostgreSQL instance is set to 'on'  
**Description:***Enabling the log\_connections setting causes each attempted connection to the server to be logged, along with successful completion of client authentication. This parameter cannot be changed after the session starts.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that the 'log\_disconnections' database flag for Cloud SQL PostgreSQL instance is set to 'on'  
**Description:***Enabling the log\_disconnections setting logs the end of each session, including the session duration.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure 'log\_statement' database flag for Cloud SQL PostgreSQL instance is set appropriately  
**Description:***The value of log\_statement flag determined the SQL statements that are logged. Valid values are: 'none', 'ddl', 'mod', and 'all'.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure 'log\_hostname' database flag for Cloud SQL PostgreSQL instance is set appropriately  
**Description:***PostgreSQL logs only the IP address of the connecting hosts. The log\_hostname flag controls the logging of hostnames in addition to the IP addresses logged. The performance hit is dependent on the configuration of the environment and the host name resolution setup. This parameter can only be set in the postgresql.conf file or on the server command line.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that the 'log\_min\_messages' database flag for Cloud SQL PostgreSQL instance is set appropriately  
**Description:***The log\_min\_messages flag defines the minimum message severity level that is considered as an error statement. Messages for error statements are logged with the SQL statement. Valid values include DEBUG5, DEBUG4, DEBUG3, DEBUG2, DEBUG1, INFO, NOTICE, WARNING, ERROR, LOG, FATAL, and PANIC. Each severity level includes the subsequent levels mentioned above.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Manual verification required. | Manual |

**Parent** **Control:** Ensure 'log\_min\_error\_statement' database flag for Cloud SQL PostgreSQL instance is set to 'Error' or stricter  
**Description:***The log\_min\_error\_statement flag defines the minimum message severity level that are considered as an error statement. Messages for error statements are logged with the SQL statement. Valid values include DEBUG5, DEBUG4, DEBUG3, DEBUG2, DEBUG1, INFO, NOTICE, WARNING, ERROR, LOG, FATAL, and PANIC. Each severity level includes the subsequent levels mentioned above. Ensure a value of ERROR or stricter is set.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that the 'log\_min\_duration\_statement' database flag for Cloud SQL PostgreSQL instance is set to '-1' (disabled)  
**Description:***The log\_min\_duration\_statement flag defines the minimum amount of execution time of a statement in milliseconds where the total duration of the statement is logged. Ensure that log\_min\_duration\_statement is disabled, i.e., a value of -1 is set.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure That 'cloudsql.enable\_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging  
**Description:***Ensure cloudsql.enable\_pgaudit database flag for Cloud SQL PostgreSQL instance is set to on to allow for centralized logging.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Cloud SQL Admin API has not been used in project 159775217402 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/sqladmin.googleapis.com/overview?project=159775217402"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadata": {  "consumer": "projects/159775217402"   "service": "sqladmin.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

**Parent** **Control:** Ensure that VPC Flow Logs is enabled for every subnet in a VPC Network  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

## **Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.** (NIST-DE.DP)

**NIST-DE.DP.1** Roles and responsibilities for detection are well defined to ensure accountability

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.DP.2** Detection activities comply with all applicable requirements

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.DP.3** Detection processes are tested

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.DP.4** Event detection information is communicated to appropriate parties

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-DE.DP.5** Detection processes are continuously improved

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** CloudWatch alarm should have an action configured  
**Description:***Checks if CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT\_DATA, or OK state. Optionally checks if any actions match a named ARN. The rule is non compliant if there is no action specified for the alarm or optional parameter.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game-WriteCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |
| **qa tester** | **AWS** | High-Low-Game-ReadCapacityUnitsLimit-BasicAlarm alarm action enabled. | Ok |

**Parent** **Control:** GuardDuty should be enabled  
**Description:***Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-south-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ca-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-central-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-north-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-3. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in eu-west-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in sa-east-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | No GuardDuty detector found in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region not supported. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

**Parent** **Control:** AWS Security Hub should be enabled for an AWS Account  
**Description:***AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | Security Hub disabled in us-east-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-south-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ca-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-central-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-north-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-3. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in eu-west-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-northeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in sa-east-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-1. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in ap-southeast-2. | Alarm |
| **qa tester** | **AWS** | Security Hub disabled in us-east-1. | Alarm |
| **qa tester** | **AWS** | ap-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | eu-south-1 region not supported. | Error |
| **qa tester** | **AWS** | eu-south-2 region is disabled. | Error |
| **qa tester** | **AWS** | me-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | il-central-1 region is disabled. | Error |
| **qa tester** | **AWS** | eu-central-2 region is disabled. | Error |
| **qa tester** | **AWS** | af-south-1 region not supported. | Error |
| **qa tester** | **AWS** | ap-northeast-3 region not supported. | Error |
| **qa tester** | **AWS** | me-south-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-east-1 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-3 region is disabled. | Error |
| **qa tester** | **AWS** | ap-southeast-4 region is disabled. | Error |

# Response Management

## **Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.** (NIST-RC.RP)

**NIST-RC.RP.1** Recovery plan is executed during or after a cybersecurity incident

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Backup plan min frequency and min retention check  
**Description:***Checks if a backup plan has a backup rule that satisfies the required frequency and retention period(35 Days). The rule is non compliant if recovery points are not created at least as often as the specified frequency or expire before the specified period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: e8bb8971-d9be-486c-91aa-79d8acbe99ea  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** DynamoDB table auto scaling should be enabled  
**Description:***Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game autoscaling not enabled. | Alarm |

**Parent** **Control:** DynamoDB tables should be in a backup plan  
**Description:***To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: 31b40971-8afb-440c-85fb-75653a3ffe8f  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** DynamoDB table point-in-time recovery should be enabled  
**Description:***Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game point-in-time recovery not enabled. | Alarm |

**Parent** **Control:** DynamoDB table should be protected by backup plan  
**Description:***Ensure if Amazon DynamoDB tables are protected by a backup plan. The rule is non compliant if the DynamoDB Table is not covered by a backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListProtectedResources  https response error StatusCode: 403  RequestID: 8df0f97d-d531-4e9f-aea4-af348c2be4b6  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListProtectedResources because no identity-based policy allows the backup:ListProtectedResources action (SQLSTATE HV000) | Error |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

## **Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.** (NIST-RC.IM)

**NIST-RC.IM.1** Recovery plans incorporate lessons learned

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RC.IM.2** Recovery strategies are updated

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).** (NIST-RC.CO)

**NIST-RC.CO.1** Public relations are managed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RC.CO.2** Reputation after an event is repaired

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RC.CO.3** Recovery activities are communicated to internal stakeholders and executive and management teams

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.** (NIST-RS.RP)

**NIST-RS.RP.1** Response plan is executed during or after an incident

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Backup plan min frequency and min retention check  
**Description:***Checks if a backup plan has a backup rule that satisfies the required frequency and retention period(35 Days). The rule is non compliant if recovery points are not created at least as often as the specified frequency or expire before the specified period.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: e8bb8971-d9be-486c-91aa-79d8acbe99ea  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** DynamoDB table auto scaling should be enabled  
**Description:***Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game autoscaling not enabled. | Alarm |

**Parent** **Control:** DynamoDB tables should be in a backup plan  
**Description:***To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListBackupPlans  https response error StatusCode: 403  RequestID: 31b40971-8afb-440c-85fb-75653a3ffe8f  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListBackupPlans because no identity-based policy allows the backup:ListBackupPlans action (SQLSTATE HV000) | Error |

**Parent** **Control:** DynamoDB table point-in-time recovery should be enabled  
**Description:***Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | High-Low-Game point-in-time recovery not enabled. | Alarm |

**Parent** **Control:** DynamoDB table should be protected by backup plan  
**Description:***Ensure if Amazon DynamoDB tables are protected by a backup plan. The rule is non compliant if the DynamoDB Table is not covered by a backup plan.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | operation error Backup: ListProtectedResources  https response error StatusCode: 403  RequestID: 8df0f97d-d531-4e9f-aea4-af348c2be4b6  api error AccessDeniedException: User: arn:aws:iam::986601184113:user/cytexaudit is not authorized to perform: backup:ListProtectedResources because no identity-based policy allows the backup:ListProtectedResources action (SQLSTATE HV000) | Error |

**Parent** **Control:** S3 bucket cross-region replication should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | testing177 not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | cytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstfintech not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | bstlegal not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | edmsnapshots not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | entjedi not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | prytex not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | jediar not enabled with cross-region replication. | Alarm |
| **qa tester** | **AWS** | devicedetector not enabled with cross-region replication. | Alarm |

**Parent** **Control:** S3 bucket versioning should be enabled  
**Description:***Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **qa tester** | **AWS** | jediar versioning disabled. | Alarm |
| **qa tester** | **AWS** | cytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | devicedetector versioning disabled. | Alarm |
| **qa tester** | **AWS** | prytex versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstlegal versioning disabled. | Alarm |
| **qa tester** | **AWS** | entjedi versioning disabled. | Alarm |
| **qa tester** | **AWS** | usdztestingbucket versioning disabled. | Alarm |
| **qa tester** | **AWS** | edmsnapshots versioning disabled. | Alarm |
| **qa tester** | **AWS** | testing177 versioning disabled. | Alarm |
| **qa tester** | **AWS** | bstfintech versioning enabled. | Ok |

## **Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).** (NIST-RS.CO)

**NIST-RS.CO.1** Personnel know their roles and order of operations when a response is needed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.CO.2** Incidents are reported consistent with established criteria

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.CO.3** Information is shared consistent with response plans

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.CO.4** Coordination with stakeholders occurs consistent with response plans

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.CO.5** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Ensure That 'All users with the following roles' is set to 'Owner'  
**Description:***Enable security alert emails to subscription owners.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | "All users with the following roles" not set to Owner. | Alarm |

**Parent** **Control:** Ensure 'Additional email addresses' is Configured with a Security Contact Email  
**Description:***Microsoft Defender for Cloud emails the subscription owners whenever a high-severity alert is triggered for their subscription. You should provide a security contact email address as an additional email address.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **SQAE** | **Azure** | Additional email addresses not configured. | Alarm |

## **Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities** (NIST-RS.AN)

**NIST-RS.AN.1** Notifications from detection systems are investigated

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.AN.2** The impact of the incident is understood

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.AN.3** Forensics are performed

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.AN.4** Incidents are categorized consistent with response plans

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.AN.5** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**Automated scan results:**   
**Parent** **Control:** Ensure that sinks are configured for all log entries  
**Description:***It is recommended to create a sink that will export copies of all the log entries. This can help aggregate logs from multiple projects and export them to a Security Information and Event Management (SIEM).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | Sinks not configured for all log entries. | Alarm |

**Parent** **Control:** Ensure that Cloud DNS logging is enabled for all VPC networks  
**Description:***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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Account Name** | **Asset** | **Result** | **Status** |
| **QA tester** | **Gcp** | googleapi: Error 403: Compute Engine API has not been used in project cytex-85fe6 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6 then retry. If you enabled this API recently  wait a few minutes for the action to propagate to our systems and retry. Details: [  {  "@type": "type.googleapis.com/google.rpc.Help"   "links": [  {  "description": "Google developers console API activation"   "url": "https://console.developers.google.com/apis/api/compute.googleapis.com/overview?project=cytex-85fe6"  }  ]  }   {  "@type": "type.googleapis.com/google.rpc.ErrorInfo"   "domain": "googleapis.com"   "metadatas": {  "consumer": "projects/cytex-85fe6"   "service": "compute.googleapis.com"  }   "reason": "SERVICE\_DISABLED"  } ]   accessNotConfigured (SQLSTATE HV000) | Error |

## **Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.** (NIST-RS.MI)

**NIST-RS.MI.1** Incidents are contained

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.MI.2** Incidents are mitigated

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.MI.3** Newly identified vulnerabilities are mitigated or documented as accepted risks

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

## **Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.** (NIST-RS.IM)

**NIST-RS.IM.1** Response plans incorporate lessons learned

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

**NIST-RS.IM.2** Response strategies are updated

**Guidance:** *No guidance available.*

**Attestation Statement:** *No attestation statement given.*

***Auditor’s Feedback:*** *No auditor feedback given.*

**Attached Files:** *No files are attached.*

# Recommendations *Recommendations goes here.*