CyberHAT Security Team

Security audit of AWS infrastructure for ticketing system prod environment

ACCESSANALYZER

ACCESSANALYZER ENABLED

Description: Check if IAM Access Analyzer is enabled

Remediation: Enable IAM Access Analyzer for all accounts, create analyzer and take action over it is recommendations (IAM Access Analyzer is available at no additional cost).

```
aws accessanalyzer create-analyzer --analyzer-name <NAME>
--type <ACCOUNT|ORGANIZATION>
```

Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html

Risk: AWS IAM Access Analyzer helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, that are shared with an external entity. This lets you identify unintended access to your resources and data, which is a security risk. IAM Access Analyzer uses a form of mathematical analysis called automated reasoning, which applies logic and mathematical inference to determine all possible access paths allowed by a resource policy.

Severity: low

IAM Access Analyzer in account {ACCOUNT ID REDACTED} is not enabled.

- arn:aws:iam::{ARN REDACTED}

ATHENA WORKGROUP ENCRYPTION

Description: Ensure that encryption at rest is enabled for Amazon Athena query results stored in Amazon S3 in order to secure data and meet compliance requirements for data-at-rest encryption.

Remediation: Enable Encryption. Use a CMK where possible. It will provide additional management and privacy benefits.

```
aws athena update-work-group --region <REGION> --work-group
<workgroup_name> --configuration-updates
ResultConfigurationUpdates={EncryptionConfiguration={Encryp
tionOption=SSE_S3|SSE_KMS|CSE_KMS}}
```

Reference:
https://docs.aws.amazon.com/athena/latest/ug/encrypting-query-results-stored-in-s3.html

Risk: If not enabled sensitive information at rest is not protected.

Severity: medium

Athena WorkGroup primary does not encrypt the query results.

- arn:aws:athena:ap-northeast-1:{ARN REDACTED}
- arn:aws:athena:ap-northeast-2:{ARN REDACTED}
- arn:aws:athena:ap-northeast-3:{ARN REDACTED}
- arn:aws:athena:ap-south-1:{ARN REDACTED}
- arn:aws:athena:ap-southeast-1:{ARN REDACTED}
- arn:aws:athena:ap-southeast-2:{ARN REDACTED}
- arn:aws:athena:ca-central-1:{ARN REDACTED}
- arn:aws:athena:eu-central-1:{ARN REDACTED}
- arn:aws:athena:eu-north-1:{ARN REDACTED}
- arn:aws:athena:eu-west-1{ARN REDACTED}
- arn:aws:athena:eu-west-2:{ARN REDACTED}
- arn:aws:athena:eu-west-3:{ARN REDACTED}
- arn:aws:athena:sa-east-1:{ARN REDACTED}
- arn:aws:athena:us-east-1:{ARN REDACTED}
- arn:aws:athena:us-east-2:{ARN REDACTED}
- arn:aws:athena:us-west-1:{ARN REDACTED}
- arn:aws:athena:us-west-2:{ARN REDACTED}

ATHENA WORKGROUP ENFORCE CONFIGURATION

Description: Ensure that workgroup configuration is enforced so it cannot be overriden by client-side settings.

Remediation: Ensure that workgroup configuration is enforced so it cannot be overriden by client-side settings.

```
aws athena update-work-group --region <REGION> --work-group
<workgroup_name> --configuration-updates
EnforceWorkGroupConfiguration=True
```

Reference:
https://docs.aws.amazon.com/athena/latest/ug/workgroups-settings-override.html

Risk: If workgroup configuration is not enforced security settings like encryption can be overriden by client-side settings.

Severity: medium

Athena WorkGroup primary does not enforce the workgroup configuration, so it can be overridden by the client-side settings.

- arn:aws:athena:ap-northeast-1:{ARN REDACTED}
- arn:aws:athena:ap-northeast-2:{ARN REDACTED}
- arn:aws:athena:ap-northeast-3:{ARN REDACTED}
- arn:aws:athena:ap-south-1:{ARN REDACTED}
- arn:aws:athena:ap-southeast-1:{ARN REDACTED}
- arn:aws:athena:ap-southeast-2:{ARN REDACTED}
- arn:aws:athena:ca-central-1:{ARN REDACTED}
- arn:aws:athena:eu-central-1:{ARN REDACTED}
- arn:aws:athena:eu-north-1:{ARN REDACTED}
- arn:aws:athena:eu-west-1:{ARN REDACTED}
- arn:aws:athena:eu-west-2:{ARN REDACTED}
- arn:aws:athena:eu-west-3:{ARN REDACTED}
- arn:aws:athena:sa-east-1:{ARN REDACTED}
- arn:aws:athena:us-east-1:{ARN REDACTED}
- arn:aws:athena:us-east-2:{ARN REDACTED}
- arn:aws:athena:us-west-1:{ARN REDACTED}
- arn:aws:athena:us-west-2:{ARN REDACTED}

AUTOSCALING

AUTOSCALING GROUP MULTIPLE AZ

Description: EC2 Auto Scaling Group should use multiple Availability Zones

Remediation: Configure multiple Availability Zones for EC2 Auto Scaling Group

```
aws autoscaling update-auto-scaling-group
```

Reference:
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html

Risk: In case of a failure in a single Availability Zone, the Auto Scaling Group will not be able to launch new instances to replace the failed ones.

Severity: medium

Autoscaling group extra has only one availability zones.

- arn:aws:autoscaling:eu-central-1:{ARN REDACTED}

Autoscaling group prometheus has only one availability zones.

- arn:aws:autoscaling:eu-central-1:{ARN REDACTED}

BACKUP

BACKUP VAULTS EXIST

Description: This check ensures that AWS Backup vaults exist to provide a secure and durable storage location for backup data.

Remediation: Use AWS Backup to create backup vaults for your critical data and services.

```
aws backup create-backup-vault --backup-vault-name
<backup_vault_name>
```

Reference:
https://docs.aws.amazon.com/aws-backup/latest/devguide/vaults.html

Risk: Without an AWS Backup vault, an organization's critical data may be at risk of being lost in the event of an accidental deletion, system failures, or natural disasters.

Severity: low

No Backup Vault exist.

- arn:aws:iam::{ARN REDACTED}

CLOUDFRONT

CLOUDFRONT DISTRIBUTIONS FIELD LEVEL ENCRYPTION ENABLED

Description: Check if CloudFront distributions have Field Level Encryption enabled.

Remediation: Check if applicable to any sensitive data. This encryption ensures that only applications that need the data—and have the credentials to decrypt it - are able to do so.

https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/CloudFront/field-level-encryption-enabled.html

Reference: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html

Risk: Allows you protect specific data throughout system processing so that only certain applications can see it.

Severity: low

CloudFront Distribution E3G6KIH8FAXFIM has Field Level Encryption disabled.

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution E1OO725IRVH0S0 has Field Level Encryption disabled.

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution EVU1YI37GOEZO has Field Level Encryption disabled.

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution E3K3CYG6OP7GSM has Field Level Encryption disabled.

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution E3B3TSXAAFXPYR has Field Level Encryption disabled.

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CLOUDFRONT DISTRIBUTIONS LOGGING ENABLED

Description: Check if CloudFront distributions have logging enabled.

Remediation: Real-time monitoring can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. Enable logging for services with defined log rotation. These logs are useful for Incident Response and forensics investigation among other use cases.

https://docs.bridgecrew.io/docs/logging_20#cli-command

Reference: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

Risk: If not enabled monitoring of service use is not possible.

Severity: medium

CloudFront Distribution {CloudFront Distribution REDACTED} **has logging disabled.**

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution {CloudFront Distribution REDACTED} **has logging disabled.**

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution {CloudFront Distribution REDACTED} **has logging disabled.**

- arn:aws:cloudfront:{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution {CloudFront Distribution REDACTED} **has logging disabled.**

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution {CloudFront Distribution REDACTED} **has logging disabled.**

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CLOUDFRONT DISTRIBUTIONS USING WAF

Description: Check if CloudFront distributions are using WAF.

Remediation: Use AWS WAF to protect your service from common web exploits. These could affect availability and performance; compromise security; or consume excessive resources.

https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/CloudFront/cloudfront-integrated-with-waf.html

Reference: https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html

Risk: Potential attacks and / or abuse of service; more even for even for internet reachable services.

Severity: medium

CloudFront Distribution {CloudFront Distribution REDACTED} **is not using AWS WAF web ACL.**

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution {CloudFront Distribution REDACTED} **is not using AWS WAF web ACL.**

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution {CloudFront Distribution REDACTED} **is not using AWS WAF web ACL.**

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution {CloudFront Distribution REDACTED} **is not using AWS WAF web ACL.**

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CloudFront Distribution {CloudFront Distribution REDACTED} **is not using AWS WAF web ACL.**

- arn:aws:cloudfront::{ARN REDACTED}:distribution/{ARN REDACTED}

CLOUDTRAIL

CLOUDTRAIL MULTI REGION ENABLED

Description: Ensure CloudTrail is enabled in all regions

Remediation: Ensure Logging is set to ON on all regions (even if they are not being used at the moment.

```
aws cloudtrail create-trail --name <trail_name>
--bucket-name <s3_bucket_for_cloudtrail>
--is-multi-region-trail aws cloudtrail update-trail --name
<trail_name> --is-multi-region-trail
```

Reference:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrailconcepts.html#cloudtrail-concepts-management-events

Risk: AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded 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 the AWS service.

Severity: high

No CloudTrail trails enabled and logging were found.

- arn:aws:iam::{ARN REDACTED}

CLOUDTRAIL MULTI REGION ENABLED LOGGING MANAGEMENT EVENTS

Description: Ensure CloudTrail logging management events in All Regions

Remediation: Enable CloudTrail logging management events in All Regions

```
aws cloudtrail update-trail --name <trail_name>
--is-multi-region-trail
```

Reference:
https://docs.bridgecrew.io/docs/logging_14

Risk: AWS CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. To meet FTR requirements, you must have management events enabled for all AWS accounts and in all regions and aggregate these logs into an Amazon Simple Storage Service (Amazon S3) bucket owned by a separate AWS account.

Severity: low

No trail found with multi-region enabled and logging management events.

- arn:aws:iam::{ARN REDACTED}

CLOUDTRAIL S3 DATAEVENTS READ ENABLED

Description: Ensure that all your AWS CloudTrail trails are configured to log Data events in order to record S3 object-level API operations, such as GetObject, DeleteObject and PutObject, for individual S3 buckets or for all current and future S3 buckets provisioned in your AWS account.

Remediation: Enable logs. Create an S3 lifecycle policy. Define use cases, metrics and automated responses where applicable.

```
aws cloudtrail put-event-selectors --trail-name
<YOUR_TRAIL_NAME_HERE> --event-selectors '[{
'ReadWriteType': 'ReadOnly',
'IncludeManagementEvents':true, 'DataResources': [{ 'Type':
'AWS::S3::Object', 'Values': ['arn:aws:s3'] }] }]'
```

Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/enable-cloudtrail-logging-for-s3.html

Risk: If logs are not enabled, monitoring of service use and threat analysis is not possible.

Severity: low

No CloudTrail trails have a data event to record all S3 object-level API operations.

- arn:aws:iam::{ARN REDACTED}

CLOUDTRAIL S3 DATAEVENTS WRITE ENABLED

Description: Ensure that all your AWS CloudTrail trails are configured to log Data events in order to record S3 object-level API operations, such as GetObject, DeleteObject and PutObject, for individual S3 buckets or for all current and future S3 buckets provisioned in your AWS account.

Remediation: Enable logs. Create an S3 lifecycle policy. Define use cases, metrics and automated responses where applicable.

```
aws cloudtrail put-event-selectors --trail-name
<YOUR_TRAIL_NAME_HERE> --event-selectors '[{
'ReadWriteType': 'WriteOnly',
'IncludeManagementEvents':true, 'DataResources': [{ 'Type':
'AWS::S3::Object', 'Values': ['arn:aws:s3'] }] }]'
```

Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/enable-cloudtrail-logging-for-s3.html

Risk: If logs are not enabled, monitoring of service use and threat analysis is not possible.

Severity: low

No CloudTrail trails have a data event to record all S3 object-level API operations.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH

CLOUDWATCH CHANGES TO NETWORK ACLS ALARM CONFIGURED

Description: Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL).

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_11#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH CHANGES TO NETWORK GATEWAYS ALARM CONFIGURED

Description: Ensure a log metric filter and alarm exist for changes to network gateways.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_12#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH CHANGES TO NETWORK ROUTE TABLES ALARM CONFIGURED

Description: Real-time monitoring of API calls can be achieved by directing Cloud Trail Logs to CloudWatch Logs, or an external Security information and event management (SIEM)environment, and establishing corresponding metric filters and alarms. Routing tablesare used to route network traffic between subnets and to network gateways. It isrecommended that a metric filter and alarm be established for changes to route tables.

Remediation: If you are using CloudTrails and CloudWatch, perform the following to setup the metric filter, alarm, SNS topic, and subscription:

1. Create a metric filter based on filter pattern provided which checks for route table changes and the <cloudtrail_log_group_name> taken from audit step 1.

```
aws logs put-metric-filter --log-group-name <cloudtrail_log_group_name> --
filter-name `<route_table_changes_metric>` --metric-transformations
metricName= `<route_table_changes_metric>`
,metricNamespace='CISBenchmark',metricValue=1 --filter-pattern '{
($.eventName = CreateRoute) || ($.eventName = CreateRouteTable) ||
($.eventName = ReplaceRoute) || ($.eventName =
ReplaceRouteTableAssociation) || ($.eventName = DeleteRouteTable) ||
($.eventName = DeleteRoute) || ($.eventName = DisassociateRouteTable) }'
```

Note: You can choose your own metricName and metricNamespace strings. Using the same metricNamespace for all Foundations Benchmark metrics will group them together.

2. Create an SNS topic that the alarm will notify aws sns create-topic --name <sns_topic_name>

Note: you can execute this command once and then re-use the same topic for all monitoring alarms.

3. Create an SNS subscription to the topic created in step 2

```
aws sns subscribe --topic-arn <sns_topic_arn> --protocol <protocol_for_sns>
- -notification-endpoint <sns_subscription_endpoints>
```

Note: you can execute this command once and then re-use the SNS subscription for all monitoring alarms.

4. Create an alarm that is associated with the CloudWatch Logs Metric Filter created in step 1 and an SNS topic created in step 2

```
aws cloudwatch put-metric-alarm --alarm-name
`<route_table_changes_alarm>` --metric-name
`<route_table_changes_metric>` --statistic Sum --period 300 - -threshold 1
--comparison-operator GreaterThanOrEqualToThreshold -- evaluation-periods
1 --namespace 'CISBenchmark' --alarm-actions <sns_topic_arn>
```

https://docs.bridgecrew.io/docs/monitoring_13#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: CloudWatch is an AWS native service that allows you to ob serve and monitor resources and applications. CloudTrail Logs can also be sent to an external Security informationand event management (SIEM) environment for monitoring and alerting.Monitoring changes to route tables will help ensure that all VPC traffic flows through anexpected path and prevent any accidental or intentional modifications that may lead touncontrolled network traffic. An alarm should be triggered every time an AWS API call isperformed to create, replace, delete, or disassociate a Route Table.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH CHANGES TO VPCS ALARM CONFIGURED

Description: Ensure a log metric filter and alarm exist for VPC changes.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_14#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG GROUP KMS ENCRYPTION ENABLED

Description: Check if CloudWatch log groups are protected by AWS KMS.

Remediation: Associate KMS Key with Cloudwatch log group.

```
associate-kms-key --log-group-name <value> --kms-key-id
<value>
```

Reference: https://docs.aws.amazon.com/cli/latest/reference/logs/associate-kms-key.html

Risk: Using customer managed KMS to encrypt CloudWatch log group provide additional confidentiality and control over the log data.

Severity: medium

Log Group {LOG GROUP NAME REDACTED} does not have AWS KMS keys associated.

- arn:aws:logs:eu-central-1:{ARN REDACTED}

Log Group {LOG GROUP NAME REDACTED} does not have AWS KMS keys associated.

- arn:aws:logs:eu-central-1:{ARN REDACTED}

CLOUDWATCH LOG GROUP RETENTION POLICY SPECIFIC DAYS ENABLED

Description: Check if CloudWatch Log Groups have a retention policy of specific days.

Remediation: Add Log Retention policy of specific days to log groups. This will persist logs and traces for a long time.

https://docs.bridgecrew.io/docs/logging_13#cli-command

Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/AWS_Logs.html

Risk: If log groups have a low retention policy of less than specific days, crucial logs and data can be lost.

Severity: medium

Log Group {LOG GROUP NAME REDACTED} has less than 365 days retention period (90 days).

- arn:aws:logs:eu-central-1:{ARN REDACTED}

Log Group {LOG GROUP NAME REDACTED} has less than 365 days retention period (90 days).

- arn:aws:logs:eu-central-1:{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER AND ALARM FOR AWS CONFIG CONFIGURATION CHANGES ENABLED

Description: Ensure a log metric filter and alarm exist for AWS Config configuration changes.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_9#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER AND ALARM FOR CLOUDTRAIL CONFIGURATION CHANGES ENABLED

Description: Ensure a log metric filter and alarm exist for CloudTrail configuration changes.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_5#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER AUTHENTICATION FAILURES

Description: Ensure a log metric filter and alarm exist for AWS Management Console authentication failures.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_6#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER AWS ORGANIZATIONS CHANGES

Description: Ensure a log metric filter and alarm exist for AWS Organizations changes.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER DISABLE OR SCHEDULED DELETION OF KMS CMK

Description: Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created KMS CMKs.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_7#procedure

Reference:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER FOR S3 BUCKET POLICY CHANGES

Description: Ensure a log metric filter and alarm exist for S3 bucket policy changes.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_8#procedure

Reference:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER POLICY CHANGES

Description: Ensure a log metric filter and alarm exist for IAM policy changes.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_4#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER ROOT USAGE

Description: Ensure a log metric filter and alarm exist for usage of root account.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_3#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER SECURITY GROUP CHANGES

Description: Ensure a log metric filter and alarm exist for security group changes.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_10#procedure

Reference:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER SIGN IN WITHOUT MFA

Description: Ensure a log metric filter and alarm exist for Management Console sign-in without MFA.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_2#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CLOUDWATCH LOG METRIC FILTER UNAUTHORIZED API CALLS

Description: Ensure a log metric filter and alarm exist for unauthorized API calls.

Remediation: It is recommended that a metric filter and alarm be established for unauthorized requests.

https://docs.bridgecrew.io/docs/monitoring_1#procedure

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Risk: Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Severity: medium

No CloudWatch log groups found with metric filters or alarms associated.

- arn:aws:iam::{ARN REDACTED}

CONFIG

CONFIG RECORDER ALL REGIONS ENABLED

Description: Ensure AWS Config is enabled in all regions.

Remediation: It is recommended to enable AWS Config in all regions.

`https://docs.bridgecrew.io/docs/logging_5-enable-aws-config-regions#cli-command`

Reference:
https://aws.amazon.com/blogs/mt/aws-config-best-practices/

Risk: The AWS configuration item history captured by AWS Config enables security analysis, resource change tracking and compliance auditing.

Severity: medium

AWS Config recorder {ID REDACTED} is disabled.

- arn:aws:iam::{ARN REDACTED}

EC2

EC2 EBS DEFAULT ENCRYPTION

Description: Check if EBS Default Encryption is activated.

Remediation: Enable Encryption. Use a CMK where possible. It will provide additional management and privacy benefits.

```
aws ec2 enable-ebs-encryption-by-default
```

Reference:
https://aws.amazon.com/premiumsupport/knowledge-center/ebs-automatic-encryption/

Risk: If not enabled sensitive information at rest is not protected.

Severity: medium

EBS Default Encryption is not activated.

- arn:aws:iam::{ARN REDACTED}

EC2 EBS VOLUME ENCRYPTION

Description: Ensure there are no EBS Volumes unencrypted.

Remediation: Encrypt all EBS volumes and Enable Encryption by default You can configure your AWS account to enforce the encryption of the new EBS volumes and snapshot copies that you create. For example; Amazon EBS encrypts the EBS volumes created when you launch an instance and the snapshots that you copy from an unencrypted snapshot.

Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

Risk: Data encryption at rest prevents data visibility in the event of its unauthorized access or theft.

Severity: medium

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EBS Snapshot {VOLUME REDACTED} is unencrypted.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 EBS VOLUME SNAPSHOTS EXISTS

Description: Check if EBS snapshots exists.

Remediation: Creating point-in-time EBS snapshots periodically will allow you to handle efficiently your data recovery process in the event of a failure, to save your data before shutting down an EC2 instance, to back up data for geographical expansion and to maintain your disaster recovery stack up to date.

```
aws ec2 --region <REGION> create-snapshot --volume-id
<VOLUME-ID>
```

Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

Risk: Ensure that your EBS volumes (available or in-use) have recent snapshots (taken weekly) available for point-in-time recovery for a better, more reliable data backup strategy.

Severity: medium

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume{VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Snapshots not found for the EBS volume {VOLUME REDACTED}.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 INSTANCE MANAGED BY SSM

Description: Check if EC2 instances are managed by Systems Manager.

Remediation: Verify and apply Systems Manager Prerequisites.

Reference:
https://docs.aws.amazon.com/systems-manager/latest/userguide/managed_instances.html

Risk: AWS Config provides AWS Managed Rules, which are predefined, customizable rules that AWS Config uses to evaluate whether your AWS resource configurations comply with common best practices.

Severity: medium

EC2 Instance {INSTANCE ID REDACTED} is not managed by Systems Manager.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 Instance {INSTANCE ID REDACTED} is not managed by Systems Manager.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 Instance {INSTANCE ID REDACTED} is not managed by Systems Manager.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 Instance {INSTANCE ID REDACTED} is not managed by Systems Manager.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 Instance {INSTANCE ID REDACTED} is not managed by Systems Manager.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 Instance {INSTANCE ID REDACTED} is not managed by Systems Manager.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 Instance {INSTANCE ID REDACTED} is not managed by Systems Manager.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 Instance {INSTANCE ID REDACTED} is not managed by Systems Manager.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 NETWORK ACL ALLOW INGRESS ANY PORT

Description: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to any port.

Remediation: Apply Zero Trust approach. Implement a process to scan and remediate unrestricted or overly permissive network acls. Recommended best practices is to narrow the definition for the minimum ports required.

Reference:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Risk: Even having a perimeter firewall, having network acls open allows any user or malware with vpc access to scan for well known and sensitive ports and gain access to instance.

Severity: medium

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:ap-northeast-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:ap-northeast-3:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:ap-south-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:ap-southeast-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:ap-southeast-2:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:ca-central-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:eu-north-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:eu-west-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:eu-west-2:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:eu-west-3:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:sa-east-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:us-east-2:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:us-west-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has every port open to the Internet.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

EC2 NETWORK ACL ALLOW INGRESS TCP PORT 22

Description: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to SSH port 22

Remediation: Apply Zero Trust approach. Implement a process to scan and remediate unrestricted or overly permissive network acls. Recommended best practices is to narrow the definition for the minimum ports required.

Reference:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Risk: Even having a perimeter firewall, having network acls open allows any user or malware with vpc access to scan for well known and sensitive ports and gain access to instance.

Severity: medium

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:ap-northeast-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:ap-northeast-3:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:ap-south-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:ap-southeast-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:ap-southeast-2:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:ca-central-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:eu-north-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:eu-west-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:eu-west-2:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:eu-west-3:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:sa-east-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:us-east-2:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:us-west-1:{ARN REDACTED}

Network ACL {ACL ID REDACTED} has SSH port 22 open to the Internet.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

EC2 SECURITYGROUP ALLOW INGRESS FROM INTERNET TO ANY PORT

Description: Ensure no security groups allow ingress from 0.0.0.0/0 or ::/0 to any port.

Remediation: Use a Zero Trust approach. Narrow ingress traffic as much as possible. Consider north-south as well as east-west traffic.

Reference:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Risk: If Security groups are not properly configured the attack surface is increased.

Severity: high

Security group {SECURITY GROUP ID REDACTED} has all ports open to the Internet.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EC2 SECURITY GROUP DEFAULT RESTRICT TRAFFIC

Description: Ensure the default security group of every VPC restricts all traffic.

Remediation: Apply Zero Trust approach. Implement a process to scan and remediate unrestricted or overly permissive security groups. Recommended best practices is to narrow the definition for the minimum ports required.

Reference:
https://docs.aws.amazon.com/eks/latest/userguide/sec-group-reqs.html

Risk: Even having a perimeter firewall, having security groups open allows any user or malware with vpc access to scan for well known and sensitive ports and gain access to instance.

Severity: high

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:ap-northeast-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:ap-northeast-3:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:ap-south-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:ap-southeast-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:ap-southeast-2:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:ca-central-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:eu-north-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:eu-west-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:eu-west-2:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:eu-west-3:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:sa-east-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:us-east-2:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:us-west-1:{ARN REDACTED}

Default Security Group {SECURITY GROUP ID REDACTED} rules allow traffic.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

EC2 SECURITY GROUP NOT USED

Description: Ensure there are no Security Groups not being used.

Remediation: List all the security groups and then use the cli to check if they are attached to an instance.

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/ec2-find-security-group-resources/

Risk: Having clear definition and scope for Security Groups creates a better administration environment.

Severity: low

Security group {SECURITY GROUP ID REDACTED} it is not being used.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

EKS

EKS CONTROL PLANE LOGGING ALL TYPES ENABLED

Description: Ensure EKS Control Plane Audit Logging is enabled for all log types

Remediation: Make sure you logging for EKS control plane is enabled.

```
aws eks update-cluster-config --region <region_name> --name
<cluster_name> --logging
'{"clusterLogging":[{"types":["api","audit","authenticator"
,"controllerManager","scheduler"],"enabled":true}]}'
```

Reference:
https://docs.aws.amazon.com/eks/latest/userguide/logging-monitoring.html

Risk: If logs are not enabled; monitoring of service use and threat analysis is not possible.

Severity: medium

Control plane logging enabled but not all log types collected for EKS cluster prod.

- arn:aws:eks:eu-central-1:{ARN REDACTED}

ELBV2

ELBV2 DELETION PROTECTION

Description: Check if Elastic Load Balancers have deletion protection enabled.

Remediation: Enable deletion protection attribute, this is not enabled by default.

```
aws elbv2 modify-load-balancer-attributes
--load-balancer-arn <lb_arn> --attributes
Key=deletion_protection.enabled,Value=true
```

Reference:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/application-load-balancers.html#deletion-protection

Risk: If deletion protection is not enabled, the resource is not protected against deletion.

Severity: medium

ELBv2 {ELBv2 ID REDACTED} does not have deletion protection enabled.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 {ELBv2 ID REDACTED} does not have deletion protection enabled.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 {ELBv2 ID REDACTED} does not have deletion protection enabled.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 {ELBv2 ID REDACTED} does not have deletion protection enabled.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 {ELBv2 ID REDACTED} does not have deletion protection enabled.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 {ELBv2 ID REDACTED} does not have deletion protection enabled.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBV2 DESYNC MITIGATION MODE

Description: Check whether the Application Load Balancer is configured with strictest desync mitigation mode, if not check if at least is configured with the drop_invalid_header_fields attribute

Remediation: Ensure Application Load Balancer is configured with strictest desync mitigation mode or with the drop_invalid_header_fields attribute enabled

```
aws elbv2 modify-load-balancer-attributes
--load-balancer-arn <alb arn> --attributes
Key=routing.http.desync_mitigation_mode,Value=<defensive/st
rictest>
```

Reference:
https://aws.amazon.com/about-aws/whats-new/2020/08/application-and-classic-load-balancers-adding-defense-in-depth-with-introduction-of-desync-mitigation-mode/

Risk: HTTP Desync issues can lead to request smuggling and make your applications vulnerable to request queue or cache poisoning; which could lead to credential hijacking or execution of unauthorized commands.

Severity: medium

ELBv2 ALB {ELBv2 ID REDACTED} does not have desync mitigation mode set as strictest and is not dropping invalid header fields.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} does not have desync mitigation mode set as strictest and is not dropping invalid header fields.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} does not have desync mitigation mode set as strictest and is not dropping invalid header fields.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} does not have desync mitigation mode set as strictest and is not dropping invalid header fields.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBV2 INSECURE SSL CIPHERS

Description: Check if Elastic Load Balancers have insecure SSL ciphers.

Remediation: Use a Security policy with ciphers that are as strong as possible. Drop legacy and insecure ciphers.

```
aws elbv2 modify-listener --listener-arn <lb_arn>
--ssl-policy ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06
```

Reference:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html#describe-ssl-policies

Risk: Using insecure ciphers could affect privacy of in transit information.

Severity: medium

ELBv2 {ELBv2 ID REDACTED} has listeners with insecure SSL protocols or ciphers (ELBSecurityPolicy-2016-08).

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 {ELBv2 ID REDACTED} has listeners with insecure SSL protocols or ciphers (ELBSecurityPolicy-2016-08).

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 {ELBv2 ID REDACTED} has listeners with insecure SSL protocols or ciphers (ELBSecurityPolicy-2016-08).

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 {ELBv2 ID REDACTED} has listeners with insecure SSL protocols or ciphers (ELBSecurityPolicy-2016-08).

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBV2 LOGGING ENABLED

Description: Check if Elastic Load Balancers have logging enabled.

Remediation: Enable ELB logging, create a log lifecycle and define use cases.

```
aws elbv2 modify-load-balancer-attributes
--load-balancer-arn <lb_arn> --attributes
Key=access_logs.s3.enabled,Value=true
Key=access_logs.s3.bucket,Value=<bucket_name>
Key=access_logs.s3.prefix,Value=<prefix>
```

Reference:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

Risk: If logs are not enabled monitoring of service use and threat analysis is not possible.

Severity: medium

ELBv2 ALB {ELBv2 ID REDACTED} does not have access logs configured.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} does not have access logs configured.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} does not have access logs configured.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} does not have access logs configured.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} does not have access logs configured.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} does not have access logs configured.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBV2 WAF ACL ATTACHED

Description: Check if Application Load Balancer has a WAF ACL attached.

Remediation: Using the AWS Management Console open the AWS WAF console to attach an ACL.

Reference: https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-associating-aws-resource.html

Risk: If not WAF ACL is attached risk of web attacks increases.

Severity: medium

ELBv2 ALB {ELBv2 ID REDACTED} is not protected by WAF Web ACL.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} is not protected by WAF Web ACL.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} is not protected by WAF Web ACL.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

ELBv2 ALB {ELBv2 ID REDACTED} is not protected by WAF Web ACL.

- arn:aws:elasticloadbalancing:eu-central-1:{ARN REDACTED}

GUARDDUTY

GUARDDUTY IS ENABLED

Description: Check if GuardDuty is enabled

Remediation: Enable GuardDuty and analyze its findings.

https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/GuardDuty/guardduty-enabled.html

Reference:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_settingup.html

Risk: Amazon GuardDuty is a continuous security monitoring service that analyzes and processes several datasources.

Severity: medium

GuardDuty is not enabled.

- arn:aws:iam::{ARN REDACTED}

IAM

IAM AWS ATTACHED POLICY NO ADMINISTRATIVE PRIVILEGES

Description: Ensure IAM AWS-Managed policies that allow full "*:*" administrative privileges are not attached

Remediation: It is more secure to start with a minimum set of permissions and grant additional permissions as necessary; rather than starting with permissions that are too lenient and then trying to tighten them later. List policies an analyze if permissions are the least possible to conduct business activities.

https://docs.bridgecrew.io/docs/iam_47#cli-command

Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Risk: IAM policies are the means by which privileges are granted to users; groups; or roles. It is recommended and considered a standard security advice to grant least privilege—that is; granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks instead of allowing full administrative privileges. Providing full administrative privileges instead of restricting to the minimum set of permissions that the user is required to do exposes the resources to potentially unwanted actions.

Severity: high

AWS policy {POLICY NAME REDACTED} is attached and allows '*:*' administrative privileges.

- arn:aws:iam::aws:policy/{ARN REDACTED}

IAM PASSWORD POLICY EXPIRES PASSWORDS WITHIN 90 DAYS OR LESS

Description: Ensure IAM password policy expires passwords within 90 days or less

Remediation: Ensure Password expiration period (in days): is set to 90 or less.

Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Risk: Password policies are used to enforce password complexity requirements. IAM password policies can be used to ensure password are comprised of different character sets. It is recommended that the password policy require at least one uppercase letter.

Severity: medium

Password policy cannot be found.

- arn:aws:iam::{ARN REDACTED}

IAM PASSWORD POLICY LOWERCASE

Description: Ensure IAM password policy requires at least one uppercase letter

Remediation: Ensure "Requires at least one lowercase letter" is checked under "Password Policy".

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Risk: Password policies are used to enforce password complexity requirements. IAM password policies can be used to ensure password are comprised of different character sets. It is recommended that the password policy require at least one lowercase letter.

Severity: medium

Password policy cannot be found.

- arn:aws:iam::{ARN REDACTED}

IAM PASSWORD POLICY MINIMUM LENGTH 14

Description: Ensure IAM password policy requires minimum length of 14 or greater

Remediation: Ensure "Minimum password length" is checked under "Password Policy".

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Risk: Password policies are used to enforce password complexity requirements. IAM password policies can be used to ensure password are comprised of different character sets. It is recommended that the password policy require minimum length of 14 or greater.

Severity: medium

Password policy cannot be found.

- arn:aws:iam::{ARN REDACTED}

IAM PASSWORD POLICY NUMBER

Description: Ensure IAM password policy require at least one number

Remediation: Ensure "Require at least one number" is checked under "Password Policy".

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Risk: Password policies are used to enforce password complexity requirements. IAM password policies can be used to ensure password are comprised of different character sets. It is recommended that the password policy require at least one number.

Severity: medium

Password policy cannot be found.

- arn:aws:iam::{ARN REDACTED}

IAM PASSWORD POLICY REUSE 24

Description: Ensure IAM password policy prevents password reuse: 24 or greater

Remediation: Ensure "Number of passwords to remember" is set to 24.

Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Risk: Password policies are used to enforce password complexity requirements. IAM password policies can be used to ensure password are comprised of different character sets. It is recommended that the password policy prevents at least password reuse of 24 or greater.

Severity: medium

Password policy cannot be found.

- arn:aws:iam::{ARN REDACTED}

IAM PASSWORD POLICY SYMBOL

Description: Ensure IAM password policy require at least one symbol

Remediation: Ensure "Require at least one non-alphanumeric character" is checked under "Password Policy".

Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Risk: Password policies are used to enforce password complexity requirements. IAM password policies can be used to ensure password are comprised of different character sets. It is recommended that the password policy require at least one non-alphanumeric character.

Severity: medium

Password policy cannot be found.

- arn:aws:iam::{ARN REDACTED}

IAM PASSWORD POLICY UPPERCASE

Description: Ensure IAM password policy requires at least one uppercase letter

Remediation: Ensure "Requires at least one uppercase letter" is checked under "Password Policy".

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Risk: Password policies are used to enforce password complexity requirements. IAM password policies can be used to ensure password are comprised of different character sets. It is recommended that the password policy require at least one uppercase letter.

Severity: medium

Password policy cannot be found.

- arn:aws:iam::{ARN REDACTED}

IAM POLICY ATTACHED ONLY TO GROUP OR ROLES

Description: Ensure IAM policies are attached only to groups or roles

Remediation: Remove any policy attached directly to the user. Use groups or roles instead.

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Risk: By default IAM users; groups; and roles have no access to AWS resources. IAM policies are the means by which privileges are granted to users; groups; or roles. It is recommended that IAM policies be applied directly to groups and roles but not users. Assigning privileges at the group or role level reduces the complexity of access management as the number of users grow. Reducing access management complexity may in-turn reduce opportunity for a principal to inadvertently receive or retain excessive privileges.

Severity: low

User {USERNAME REDACTED} has the policy {POLICY NAME REDACTED} attached.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has the policy {POLICY NAME REDACTED} attached.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has the policy {POLICY NAME REDACTED}attached.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has the policy {POLICY NAME REDACTED} attached.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has the policy {POLICY NAME REDACTED} attached.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has the policy {POLICY NAME REDACTED} attached.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has the policy {POLICY NAME REDACTED} attached.

- arn:aws:iam::{ARN REDACTED}

IAM ROLE ADMINISTRATORACCESS POLICY

Description: Ensure IAM Roles do not have AdministratorAccess policy attached

Remediation: Apply the principle of least privilege. Instead of AdministratorAccess, assign only the permissions necessary for specific roles and tasks. Create custom IAM policies with minimal permissions based on the principle of least privilege.

Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

Risk: The AWS-managed AdministratorAccess policy grants all actions for all AWS services and for all resources in the account and as such exposes the customer to a significant data leakage threat. It should be granted very conservatively. For granting access to 3rd party vendors, consider using alternative managed policies, such as ViewOnlyAccess or SecurityAudit.

Severity: high

IAM Role {ROLE NAME REDACTED} has AdministratorAccess policy attached.

- arn:aws:iam::{ARN REDACTED}

IAM ROLE CROSS SERVICE CONFUSED DEPUTY PREVENTION

Description: Ensure IAM Service Roles prevents against a cross-service confused deputy attack

Remediation: Use the aws:SourceArn and aws:SourceAccount global condition context keys in trust relationship policies to limit the permissions that a service has to a specific resource

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/confused-deputy.html#cross-service-confused-deputy-prevention

Risk: Allow attackers to gain unauthorized access to resources

Severity: high

IAM Service Role {ROLE NAME REDACTED} does not prevent against a cross-service confused deputy attack.

- arn:aws:iam::{ARN REDACTED}

IAM Service Role {ROLE NAME REDACTED} does not prevent against a cross-service confused deputy attack.

- arn:aws:iam::{ARN REDACTED}

IAM ROTATE ACCESS KEY 90 DAYS

Description: Ensure access keys are rotated every 90 days or less

Remediation: Use the credential report to ensure access_key_X_last_rotated is less than 90 days ago.

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

Risk: Access keys consist of an access key ID and secret access key which are used to sign programmatic requests that you make to AWS. AWS users need their own access keys to make programmatic calls to AWS from the AWS Command Line Interface (AWS CLI)- Tools for Windows PowerShell- the AWS SDKs- or direct HTTP calls using the APIs for individual AWS services. It is recommended that all access keys be regularly rotated.

Severity: medium

User {USERNAME REDACTED} has not rotated access key 1 in over 90 days (205 days).

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has not rotated access key 1 in over 90 days (316 days).

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has not rotated access key 1 in over 90 days (205 days).

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has not rotated access key 1 in over 90 days (316 days).

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has not rotated access key 1 in over 90 days (321 days).

- arn:aws:iam:{ARN REDACTED}

User {USERNAME REDACTED} has not rotated access key 2 in over 90 days (321 days).

- arn:aws:iam::{ARN REDACTED}

IAM SECURITY AUDIT ROLE CREATED

Description: Ensure a Security Audit role has been created to conduct security audits

Remediation: Create an IAM role for conduct security audits with AWS.

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_security-auditor

Risk: Creating an IAM role with a security audit policy provides a clear separation of duties between the security team and other teams within the organization. This helps to ensure that security-related activities are performed by authorized individuals with the appropriate expertise and access permissions.

Severity: low

SecurityAudit policy is not attached to any role.

- arn:aws:iam::aws:policy/SecurityAudit

IAM USER ACCESS KEY UNUSED

Description: Ensure User Access Keys unused are disabled

Remediation: Find the credentials that they were using and ensure that they are no longer operational. Ideally; you delete credentials if they are no longer needed. You can always recreate them at a later date if the need arises. At the very least; you should change the password or deactivate the access keys so that the former users no longer have access.

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_finding-unused.html

Risk: To increase the security of your AWS account; remove IAM user credentials (that is; passwords and access keys) that are not needed. For example; when users leave your organization or no longer need AWS access.

Severity: medium

User {USERNAME REDACTED} has not used access key 1 in the last 45 days (51 days).

- arn:aws:iam::{ARN REDACTED}

IAM USER TWO ACTIVE ACCESS KEY

Description: Check if IAM users have two active access keys

Remediation: Avoid using long lived access keys.

Reference:
https://docs.aws.amazon.com/IAM/latest/APIReference/API_ListAccessKeys.html

Risk: Access Keys could be lost or stolen. It creates a critical risk.

Severity: medium

User {USERNAME REDACTED} has 2 active access keys.

- arn:aws:iam::{ARN REDACTED}

IAM USER WITH TEMPORARY CREDENTIALS

Description: Ensure users make use of temporary credentials assuming IAM roles

Remediation: As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys.

Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

Risk: As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys.

Severity: medium

User {USERNAME REDACTED} has long lived credentials with access to other services than IAM or STS.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has long lived credentials with access to other services than IAM or STS.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has long lived credentials with access to other services than IAM or STS.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has long lived credentials with access to other services than IAM or STS.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has long lived credentials with access to other services than IAM or STS.

- arn:aws:iam::{ARN REDACTED}

User {USERNAME REDACTED} has long lived credentials with access to other services than IAM or STS.

- arn:aws:iam::{ARN REDACTED}

INSPECTOR2

INSPECTOR2 IS ENABLED

Description: Check if Inspector2 is enabled

Remediation: Enable Inspector2

```
aws inspector2 enable
```

Reference:
https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html

Risk: Without using AWS Inspector, you may not be aware of all the security vulnerabilities in your AWS resources, which could lead to unauthorized access, data breaches, or other security incidents.

Severity: medium

Inspector2 is not enabled.

- arn:aws:inspector2:ap-northeast-1:{ARN REDACTED}

- arn:aws:inspector2:ap-northeast-2:{ARN REDACTED}
- arn:aws:inspector2:ap-northeast-3:{ARN REDACTED}
- arn:aws:inspector2:ap-south-1:{ARN REDACTED}
- arn:aws:inspector2:ap-southeast-1:{ARN REDACTED}
- arn:aws:inspector2:ap-southeast-2:{ARN REDACTED}
- arn:aws:inspector2:ca-central-1:{ARN REDACTED}
- arn:aws:inspector2:eu-central-1:{ARN REDACTED}
- arn:aws:inspector2:eu-north-1:{ARN REDACTED}
- arn:aws:inspector2:eu-west-1:{ARN REDACTED}
- arn:aws:inspector2:eu-west-2:{ARN REDACTED}
- arn:aws:inspector2:eu-west-3:{ARN REDACTED}
- arn:aws:inspector2:sa-east-1:{ARN REDACTED}
- arn:aws:inspector2:us-east-1:{ARN REDACTED}
- arn:aws:inspector2:us-east-2:{ARN REDACTED}
- arn:aws:inspector2:us-west-1:{ARN REDACTED}
- arn:aws:inspector2:us-west-2:{ARN REDACTED}

NETWORK FIREWALL

NETWORK FIREWALL IN ALL VPC

Description: Ensure all VPCs have Network Firewall enabled

Remediation: Ensure all VPCs have Network Firewall enabled

```
aws network-firewall create-firewall --firewall-name
<value> --vpc-id <value>
```

Reference:
https://docs.aws.amazon.com/network-firewall/latest/developerguide/vpc-config.html

Risk: Without a network firewall, it can be difficult to monitor and control traffic within the VPC. This can make it harder to detect and prevent attacks or unauthorized access to resources.

Severity: medium

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:ap-northeast-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:ap-northeast-3:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:ap-south-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:ap-southeast-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:ap-southeast-2:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:ca-central-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:eu-north-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:eu-west-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:eu-west-2:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:eu-west-3:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:sa-east-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:us-east-2:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:us-west-1:{ARN REDACTED}

VPC {VPC ID REDACTED} does not have Network Firewall enabled.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

RDS

RDS INSTANCE BACKUP ENABLED

Description: Check if RDS instances have backup enabled.

Remediation: Enable automated backup for production data. Define a retention period and periodically test backup restoration. A Disaster Recovery process should be in place to govern Data Protection approach.

```
aws rds modify-db-instance --db-instance-identifier
<db_instance_id> --backup-retention-period 7
--apply-immediately
```

Reference:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html

Risk: If backup is not enabled, data is vulnerable. Human error or bad actors could erase or modify data.

Severity: medium

RDS Instance {RDS ID REDACTED} does not have backup enabled.

- arn:aws:rds:eu-central-1:{ARN REDACTED}

RDS INSTANCE DELETION PROTECTION

Description: Check if RDS instances have deletion protection enabled.

Remediation: Enable deletion protection using the AWS Management Console for production DB instances.

```
aws rds modify-db-instance --db-instance-identifier
<db_instance_id> --deletion-protection --apply-immediately
```

Reference:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_DeleteInstance.html

Risk: You can only delete instances that do not have deletion protection enabled.

Severity: medium

RDS Instance {RDS ID REDACTED} deletion protection is not enabled.

- arn:aws:rds:eu-central-1:{ARN REDACTED}

RDS INSTANCE ENHANCED MONITORING ENABLED

Description: Check if RDS instances has enhanced monitoring enabled.

Remediation: To use Enhanced Monitoring, you must create an IAM role; and then enable Enhanced Monitoring.

```
aws rds create-db-instance --db-instance-identifier
<db_instance_id> --db-instance-class <instance_class>
--engine <engine> --storage-encrypted true
```

Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.OS.html

Risk: A smaller monitoring interval results in more frequent reporting of OS metrics.

Severity: low

RDS Instance {RDS ID REDACTED} does not have enhanced monitoring enabled.

- arn:aws:rds:eu-central-1:{ARN REDACTED}

RDS INSTANCE INTEGRATION CLOUDWATCH LOGS

Description: Check if RDS instances is integrated with CloudWatch Logs.

Remediation: Use CloudWatch Logs to perform real-time analysis of the log data. Create alarms and view metrics.

```
aws rds modify-db-instance --db-instance-identifier
<db_instance_id> --cloudwatch-logs-export-configuration
{'EnableLogTypes':['audit',error','general','slowquery']}
--apply-immediately
```

Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/publishing_cloudwatchlogs.html

Risk: If logs are not enabled, monitoring of service use and threat analysis is not possible.

Severity: medium

RDS Instance {RDS ID REDACTED} does not have CloudWatch Logs enabled.

- arn:aws:rds:eu-central-1:{ARN REDACTED}

RDS INSTANCE MULTI AZ

Description: Check if RDS instances have multi-AZ enabled.

Remediation: Enable multi-AZ deployment for production databases.

```
aws rds create-db-instance --db-instance-identifier
<db_instance_id> --multi-az true
```

Reference:
https://aws.amazon.com/rds/features/multi-az/

Risk: In case of failure, with a single-AZ deployment configuration, should an availability zone specific database failure occur, Amazon RDS can not automatically fail over to the standby availability zone.

Severity: medium

RDS Instance {RDS ID REDACTED} does not have multi-AZ enabled.

- arn:aws:rds:eu-central-1:{ARN REDACTED}

RDS INSTANCE STORAGE ENCRYPTED

Description: Check if RDS instances storage is encrypted.

Remediation: Enable Encryption. Use a CMK where possible. It will provide additional management and privacy benefits.

```
aws rds create-db-instance --db-instance-identifier
<db_instance_id> --db-instance-class <instance_class>
--engine <engine> --storage-encrypted true
```

Reference:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

Risk: If not enabled sensitive information at rest is not protected.

Severity: medium

RDS Instance {RDS ID REDACTED} is not encrypted.

- arn:aws:rds:eu-central-1:{ARN REDACTED}

S3

S3 ACCOUNT LEVEL PUBLIC ACCESS BLOCKS

Description: Check S3 Account Level Public Access Block.

Remediation: You can enable Public Access Block at the account level to prevent the exposure of your data stored in S3.

```
aws s3control put-public-access-block
--public-access-block-configuration
BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolic
y=true,RestrictPublicBuckets=true --account-id <account_id>
```

Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html

Risk: Public access policies may be applied to sensitive data buckets.

Severity: high

Block Public Access is not configured for the account {ACCOUNT ID REDACTED}.

- arn:aws:iam::{ARN REDACTED}

S3 BUCKET ACL PROHIBITED

Description: Check if S3 buckets have ACLs enabled

Remediation: Ensure that S3 ACLs are disabled (BucketOwnerEnforced). Use IAM policies and bucket policies to manage access.

```
aws s3api put-bucket-ownership-controls --bucket
<bucket-name> --ownership-controls
Rules=[{ObjectOwnership=BucketOwnerEnforced}]
```

Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/about-object-ownership.html

Risk: S3 ACLs are a legacy access control mechanism that predates IAM. IAM and bucket policies are currently the preferred methods.

Severity: medium

S3 Bucket {S3 BUCKET ID REDACTED} has bucket ACLs enabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has bucket ACLs enabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has bucket ACLs enabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has bucket ACLs enabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has bucket ACLs enabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has bucket ACLs enabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has bucket ACLs enabled.

- arn:aws:s3:::{ARN REDACTED}

S3 BUCKET KMS ENCRYPTION

Description: Check if S3 buckets have KMS encryption enabled.

Remediation: Ensure that S3 buckets have encryption at rest enabled using KMS.

https://www.trendmicro.com/cloudoneconformity-staging/knowledge-base/aws/S3/encrypted-with-kms-customer-master-keys.html

Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html

Risk: Amazon S3 KMS encryption provides a way to set the encryption behavior for an S3 bucket using a managed key. This will ensure data-at-rest is encrypted.

Severity: medium

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Server Side Encryption is not configured with kms for S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

S3 BUCKET LEVEL PUBLIC ACCESS BLOCK

Description: Check S3 Bucket Level Public Access Block.

Remediation: You can enable Public Access Block at the bucket level to prevent the exposure of your data stored in S3.

```
aws s3api put-public-access-block --region <REGION_NAME>
--public-access-block-configuration
BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolic
y=true,RestrictPublicBuckets=true --bucket <BUCKET_NAME>
```

Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html

Risk: Public access policies may be applied to sensitive data buckets.

Severity: medium

Block Public Access is not configured for the S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Block Public Access is not configured for the S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Block Public Access is not configured for the S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Block Public Access is not configured for the S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Block Public Access is not configured for the S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Block Public Access is not configured for the S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

Block Public Access is not configured for the S3 Bucket {S3 BUCKET ID REDACTED}.

- arn:aws:s3:::{ARN REDACTED}

S3 BUCKET NO MFA DELETE

Description: Check if S3 bucket MFA Delete is not enabled.

Remediation: Adding MFA delete to an S3 bucket, requires additional authentication when you change the version state of your bucket or you delete and object version adding another layer of security in the event your security credentials are compromised or unauthorized access is granted.

```
aws s3api put-bucket-versioning --profile my-root-profile
--bucket my-bucket-name --versioning-configuration
Status=Enabled,MFADelete=Enabled --mfa
'arn:aws:iam::00000000:mfa/root-account-mfa-device 123456'
```

Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiFactorAuthenticationDelete.html

Risk: Your security credentials are compromised or unauthorized access is granted.

Severity: medium

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has MFA Delete disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 BUCKET OBJECT LOCK

Description: Check if S3 buckets have object lock enabled

Remediation: Ensure that your Amazon S3 buckets have Object Lock feature enabled in order to prevent the objects they store from being deleted.

https://docs.bridgecrew.io/docs/ensure-that-s3-bucket-has-lock-configuration-enabled-by-default#cli-command

Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html

Risk: Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. That helps to prevent ransomware attacks.

Severity: low

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has Object Lock disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 BUCKET OBJECT VERSIONING

Description: Check if S3 buckets have object versioning enabled

Remediation: Configure versioning using the Amazon console or API for buckets with sensitive information that is changing frequently; and backup may not be enough to capture all the changes.

Reference:
https://docs.aws.amazon.com/AmazonS3/latest/dev-retired/Versioning.html

Risk: With versioning, you can easily recover from both unintended user actions and application failures.

Severity: medium

S3 Bucket {S3 BUCKET ID REDACTED} has versioning disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has versioning disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has versioning disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has versioning disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has versioning disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has versioning disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has versioning disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 BUCKET PUBLIC ACCESS

Description: Ensure there are no S3 buckets open to Everyone or Any AWS user.

Remediation: You can enable block public access settings only for access points, buckets and AWS accounts. Amazon S3 does not support block public access settings on a per-object basis. When you apply block public access settings to an account; the settings apply to all AWS Regions globally. The settings might not take effect in all Regions immediately or simultaneously, but they eventually propagate to all Regions.

```
aws s3api put-public-access-block
--public-access-block-configuration
BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolic
y=true,RestrictPublicBuckets=true --bucket <bucket_name>
```

Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html

Risk: Even if you enable all possible bucket ACL options available in the Amazon S3 console the ACL alone does not allow everyone to download objects from your bucket. Depending on which option you select any user could perform some actions.

Severity: critical

S3 Bucket {S3 BUCKET ID REDACTED} has public access due to bucket policy.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has public access due to bucket policy.

- arn:aws:s3:::{ARN REDACTED}

S3 BUCKET PUBLIC LIST ACL

Description: Ensure there are no S3 buckets listable by Everyone or Any AWS customer.

Remediation: You can enable block public access settings only for access points, buckets and AWS accounts. Amazon S3 does not support block public access settings on a per-object basis. When you apply block public access settings to an account; the settings apply to all AWS Regions globally. The settings might not take effect in all Regions immediately or simultaneously, but they eventually propagate to all Regions.

```
aws s3api put-bucket-acl --bucket <bucket_name> --acl
private
```

Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html

Risk: Even if you enable all possible bucket ACL options available in the Amazon S3 console the ACL alone does not allow everyone to download objects from your bucket. Depending on which option you select any user could perform some actions.

Severity: critical

S3 Bucket {S3 BUCKET ID REDACTED} is listable by anyone due to the bucket ACL: AllUsers having the READ permission.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} is listable by anyone due to the bucket ACL: AllUsers having the READ permission.

- arn:aws:s3:::{ARN REDACTED}

S3 BUCKET SECURE TRANSPORT POLICY

Description: Check if S3 buckets have secure transport policy.

Remediation: Ensure that S3 buckets have encryption in transit enabled.

Reference:
https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-policy-for-config-rule/

Risk: If HTTPS is not enforced on the bucket policy, communication between clients and S3 buckets can use unencrypted HTTP. As a result, sensitive information could be transmitted in clear text over the network or internet.

Severity: medium

S3 Bucket {S3 BUCKET ID REDACTED} does not have a bucket policy, thus it allows HTTP requests.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} does not have a bucket policy, thus it allows HTTP requests.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} allows requests over insecure transport in the bucket policy.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} does not have a bucket policy, thus it allows HTTP requests.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} does not have a bucket policy, thus it allows HTTP requests.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} does not have a bucket policy, thus it allows HTTP requests.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} allows requests over insecure transport in the bucket policy.

- arn:aws:s3:::{ARN REDACTED}

S3 BUCKET SERVER ACCESS LOGGING ENABLED

Description: Check if S3 buckets have server access logging enabled

Remediation: Ensure that S3 buckets have Logging enabled. CloudTrail data events can be used in place of S3 bucket logging. If that is the case, this finding can be considered a false positive.

https://docs.bridgecrew.io/docs/s3_13-enable-logging#cli-command

Reference:
https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.html

Risk: Server access logs can assist you in security and access audits; help you learn about your customer base; and understand your Amazon S3 bill.

Severity: medium

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

S3 Bucket {S3 BUCKET ID REDACTED} has server access logging disabled.

- arn:aws:s3:::{ARN REDACTED}

SECURITY HUB

SECURITY HUB ENABLED

Description: Check if Security Hub is enabled and its standard subscriptions.

Remediation: Security Hub is Regional. When you enable or disable a security standard, it is enabled or disabled only in the current Region or in the Region that you specify.

```
aws securityhub enable-security-hub
--enable-default-standards
```

Reference: https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-enable-disable.html

Risk: AWS Security Hub gives you a comprehensive view of your security alerts and security posture across your AWS accounts.

Severity: medium

Security Hub is not enabled.

- arn:aws:iam::{ARN REDACTED}

SSM

SSM INCIDENTS ENABLED WITH PLANS

Description: Ensure SSM Incidents is enabled with response plans.

Remediation: Enable SSM Incidents and create response plans

```
aws ssm-incidents create-response-plan
```

Reference: https://docs.aws.amazon.com/incident-manager/latest/userguide/response-plans.html

Risk: Not having SSM Incidents enabled can increase the risk of delayed detection and response to security incidents, unauthorized access, limited visibility into incidents and vulnerabilities

Severity: low

No SSM Incidents replication set exists.

- arn:aws:iam::{ARN REDACTED}

VPC

VPC DIFFERENT REGIONS

Description: Ensure there are VPCs in more than one region

Remediation: Ensure there are VPCs in more than one region

```
aws ec2 create-vpc
```

Reference:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-example-private-subnets-nat.html

Risk:

Severity: medium

VPCs found only in one region.

- arn:aws:iam::{ARN REDACTED}

VPC FLOW LOGS ENABLED

Description: Ensure VPC Flow Logging is Enabled in all VPCs.

Remediation: It is recommended that VPC Flow Logs be enabled for packet Rejects for VPCs.

Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html

Risk: VPC Flow Logs provide visibility into network traffic that traverses the VPC and can be used to detect anomalous traffic or insight during security workflows.

Severity: medium

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-northeast-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-northeast-3:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-south-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-southeast-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-southeast-2:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ca-central-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-north-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-west-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-west-2:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-west-3:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:sa-east-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:us-east-2:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:us-west-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

VPC PEERING ROUTING TABLES WITH LEAST PRIVILEGE

Description: Ensure routing tables for VPC peering are least access.

Remediation: Review routing tables of peered VPCs for whether they route all subnets of each VPC and whether that is necessary to accomplish the intended purposes for peering the VPCs.

https://docs.bridgecrew.io/docs/networking_5#cli-command

Reference: https://docs.aws.amazon.com/vpc/latest/peering/peering-configurations-partial-access.html

Risk: Being highly selective in peering routing tables is a very effective way of minimizing the impact of breach as resources outside of these routes are inaccessible to the peered VPC.

Severity: medium

VPC Peering Connection {PEERING ID REDACTED} does not comply with least privilege access since it accepts whole VPCs CIDR in its route tables.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC Peering Connection {PEERING ID REDACTED} does not comply with least privilege access since it accepts whole VPCs CIDR in its route tables.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC SUBNET NO PUBLIC IP BY DEFAULT

Description: Ensure VPC subnets do not assign public IP by default

Remediation: VPC subnets should not allow automatic public IP assignment

Reference: https://docs.aws.amazon.com/config/latest/developerguide/subnet-auto-assign-public-ip-disabled.html

Risk: VPC subnet is a part of the VPC having its own rules for traffic. Assigning the Public IP to the subnet automatically (on launch) can accidentally expose the instances within this subnet to internet and should be edited to 'No' post creation of the Subnet.

Severity: medium

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-3:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-3:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-northeast-3:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-south-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-south-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-south-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-southeast-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-southeast-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-southeast-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-southeast-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-southeast-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ap-southeast-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ca-central-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ca-central-1:{ARN REDACTED}

VPC subnet{SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:ca-central-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-north-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-north-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-north-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-west-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-west-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-west-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-west-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-west-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-west-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-west-3:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-west-3:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:eu-west-3:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:sa-east-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:sa-east-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:sa-east-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-east-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-east-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-east-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-west-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-west-1:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

VPC subnet {SUBNET ID REDACTED} assigns public IP by default.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

VPC SUBNET SEPARATE PRIVATE PUBLIC

Description: Ensure all VPC has public and private subnets defined

Remediation: Ensure all VPC has public and private subnets defined

```
aws ec2 create-subnet
```

Reference:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

Risk:

Severity: medium

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-northeast-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-northeast-2:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-northeast-3:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-south-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-southeast-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ap-southeast-2:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:ca-central-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-central-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-north-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-west-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-west-2:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:eu-west-3:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:sa-east-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:us-east-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:us-east-2:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:us-west-1:{ARN REDACTED}

VPC {VPC ID REDACTED} Flow logs are disabled.

- arn:aws:ec2:us-west-2:{ARN REDACTED}

WAFV2

WAFV2 WEBACL LOGGING ENABLED

Description: Check if AWS WAFv2 logging is enabled

Remediation: Enable AWS WAFv2 logging for your Web ACLs to monitor and analyze traffic patterns effectively.

```
aws wafv2 update-web-acl-logging-configuration --scope
REGIONAL --web-acl-arn
arn:partition:wafv2:region:account-id:webacl/webacl-id
--logging-configuration '{"LogDestinationConfigs":
["arn:partition:logs:region:account-id:log-group:log-group-
name"]}'
```

Reference:
https://docs.aws.amazon.com/waf/latest/developerguide/logging.html
WAFV2 WEBACL LOGGING ENABLEDWAFV2 WEBACL LOGGING ENABLED

Risk: Enabling AWS WAFv2 logging helps monitor and analyze traffic patterns for enhanced security.

Severity: medium

AWS WAFv2 Web ACL {WAFv2 Web ACL REDACTED} does not have logging enabled.

- arn:aws:wafv2:eu-central-1:{ARN REDACTED}