



Report Information

Version:

3.11.3

Parameters used:

Date:

2025-04-19T12:44:56.748210

AWS Assessment Summary

AWS Account:

390402539438

AWS-CLI Profile:

default

Audited Regions:

us-east-1

AWS Credentials

User Id:

AIDAVVZON76XCWKV27DIL

Caller Identity ARN:

arn:aws:iam::390402539438:user/prowler-user

Assessment Overview

Total Findings:

36

Passed:

2

Failed:

34

Total Resources:

3

Filters

Show

100

▼

entries

Search:

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	low	support	us-east-1	trustedadvisor_premium_support_plan_subscribed	Check if a Premium support plan is subscribed	390402539438		Amazon Web Services Premium Support Plan isn't subscribed.	Ensure that the appropriate support plan is subscribed. read more...	It is recommended that you subscribe to a support plan. read more...	
PASS	medium	cloudwatch	us-east-1	cloudwatch_cross_account_sharing_disabled	Check if CloudWatch has allowed cross-account sharing.	390402539438		CloudWatch doesn't allow cross-account sharing.	Cross-Account access to CloudW logs is not enabled. read more...	Grant usage permission on a profile. read more...	•ENS-RD2022: op.acc.4.aws.iam read more...
FAIL	low	cloudtrail	us-east-1	cloudtrail_s3_dataevents_read_enabled	Check if S3 buckets have Object-level logging for read events is enabled in CloudTrail.	390402539438		No CloudTrail trails have a data event to record all S3 object-level API operations.	If logs are not enabled, monitor S3 object-level API operations. read more...	Enable logs. Create an S3 life cycle policy. read more...	•FedRAMP-Low-Revision-4: ac-2 read more...
FAIL	low	cloudtrail	us-east-1	cloudtrail_s3_dataevents_write_enabled	Check if S3 buckets have Object-level logging for write events is enabled in CloudTrail.	390402539438		No CloudTrail trails have a data event to record all S3 object-level API operations.	If logs are not enabled, monitor S3 object-level API operations. read more...	Enable logs. Create an S3 life cycle policy. read more...	•FedRAMP-Low-Revision-4: ac-2 read more...
FAIL	high	s3	us-east-1	s3_account_level_public_access_blocks	Check S3 Account Level Public Access Block.	390402539438		Block Public Access is not configured for the account 390402539438.	Public access policies may be configured for the account. read more...	You can enable Public Access Block. read more...	•FedRAMP-Low-Revision-4: ac-3 read more...
INFO	medium	trustedadvisor	us-east-1	trustedadvisor_errors_and_warnings	Check Trusted Advisor for errors and warnings.	390402539438		Amazon Web Services Premium Support Subscription is required to use this service.	Improve the security of your account. read more...	Review and act upon its recommendations. read more...	
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_and_alarm_for_aws_config_changes_enabled	Ensure a log metric filter and alarm exist for AWS Config configuration changes.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API calls. read more...	It is recommended that a metric filter and alarm be created. read more...	•CIS-1.4: 4.9 read more... •NIST-CSF-1.1: read more...

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_authentication_failures	Ensure a log metric filter and alarm exist for AWS Management Console authentication failures.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.6 •NIST-CSF-1.1: read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_aws_organizations_changes	Ensure a log metric filter and alarm exist for AWS Organizations changes.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.15 •MITRE-ATTACK read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_changes_to_network_acls_alarm_configured	Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL).	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•FedRAMP-Low-Revision-4: ac-2 read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_changes_to_network_gateways_alarm_configured	Ensure a log metric filter and alarm exist for changes to network gateways.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•FedRAMP-Low-Revision-4: ir-4 read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_and_alarm_for_cloudtrail_configuration_changes_enabled	Ensure a log metric filter and alarm exist for CloudTrail configuration changes.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.5 •NIST-CSF-1.1: read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_disable_or_scheduled_deletion_of_kms_cmk	Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created KMS CMKs.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.7 •NIST-CSF-1.1: read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_policy_changes	Ensure a log metric filter and alarm exist for IAM policy changes.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.4 •NIST-CSF-1.1: read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_sign_in_without_mfa	Ensure a log metric filter and alarm exist for Management Console sign-in without MFA.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.2 •NIST-CSF-1.1: read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_changes_to_network_route_tables_alarm_configured	Ensure a log metric filter and alarm exist for route table changes.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•FedRAMP-Low-Revision-4: ir-4 read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_for_s3_bucket_policy_changes	Ensure a log metric filter and alarm exist for S3 bucket policy changes.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.8 •NIST-CSF-1.1: read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_security_group_changes	Ensure a log metric filter and alarm exist for security group changes.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.10 •NIST-CSF-1.1 read more...

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_unauthorized_api_calls	Ensure a log metric filter and alarm exist for unauthorized API calls.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.1 •NIST-CSF-1.1: read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_log_metric_filter_root_usage	Ensure a log metric filter and alarm exist for usage of root account.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•CIS-1.4: 4.3 •NIST-CSF-1.1: read more...
FAIL	medium	cloudwatch	us-east-1	cloudwatch_changes_to_vpcs_alarm_configured	Ensure a log metric filter and alarm exist for VPC changes.	390402539438		No CloudWatch log groups found with metric filters or alarms associated.	Monitoring unauthorized API ca read more...	It is recommended that a metri read more...	•FedRAMP-Low-Revision-4: ir-4 read more...
FAIL	low	iam	us-east-1	iam_securityaudit_role_created	Ensure a Security Audit role has been created to conduct security audits	SecurityAudit		SecurityAudit policy is not attached to any role.	Creating an IAM role with a se read more...	Create an IAM role for conduct read more...	•ENS-RD2022: op.acc.3.r2.aws. read more...
FAIL	medium	iam	us-east-1	iam_support_role_created	Ensure a support role has been created to manage incidents with AWS Support	AWSSupportServiceRolePolicy		Support policy is not attached to any role.	AWS provides a support center read more...	Create an IAM role for managin read more...	•CIS-1.4: 1.17 •ENS-RD2022: read more...
FAIL	low	backup	us-east-1	backup_vaults_exist	Ensure AWS Backup vaults exist	390402539438		No Backup Vault exist.	Without an AWS Backup vault, a read more...	Use AWS Backup to create backu read more...	•ENS-RD2022: mp.info.6.aws.bc read more...
FAIL	low	cloudtrail	us-east-1	cloudtrail_multi_region_enabled_logging_management_events	Ensure CloudTrail logging management events in All Regions	390402539438		No trail found with multi-region enabled and logging management events.	AWS CloudTrail enables governa read more...	Enable CloudTrail logging mana read more...	
FAIL	medium	iam	us-east-1	iam_password_policy_expires_passwords_within_90_days_or_less	Ensure IAM password policy expires passwords within 90 days or less	390402539438		Password policy cannot be found.	Password policies are used to read more...	Ensure Password expiration per read more...	•ISO27001-2013: A.9.2, A.9.3, read more...
FAIL	medium	iam	us-east-1	iam_password_policy_reuse_24	Ensure IAM password policy prevents password reuse: 24 or greater	390402539438		Password policy cannot be found.	Password policies are used to read more...	Ensure "Number of passwords to read more...	•CIS-1.4: 1.9 •NIST-CSF-1.1: read more...
FAIL	medium	iam	us-east-1	iam_password_policy_lowercase	Ensure IAM password policy require at least one lowercase letter	390402539438		Password policy cannot be found.	Password policies are used to read more...	Ensure "Requires at least one read more...	•GxP-21-CFR-Part-11: 11.10-d, read more...
FAIL	medium	iam	us-east-1	iam_password_policy_number	Ensure IAM password policy require at least one number	390402539438		Password policy cannot be found.	Password policies are used to read more...	Ensure "Require at least one n read more...	•GxP-21-CFR-Part-11: 11.10-d, read more...
FAIL	medium	iam	us-east-1	iam_password_policy_symbol	Ensure IAM password policy require at least one symbol	390402539438		Password policy cannot be found.	Password policies are used to read more...	Ensure "Require at least one n read more...	•GxP-21-CFR-Part-11: 11.10-d, read more...
FAIL	medium	iam	us-east-1	iam_password_policy_uppercase	Ensure IAM password policy requires at least one uppercase letter	390402539438		Password policy cannot be found.	Password policies are used to read more...	Ensure "Requires at least one read more...	•GxP-21-CFR-Part-11: 11.10-d, read more...

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recomendation	Compliance
FAIL	medium	iam	us-east-1	iam_password_policy_minimum_length_14	Ensure IAM password policy requires minimum length of 14 or greater	390402539438		Password policy cannot be found.	Password policies are used to read more...	Ensure "Minimum password lengt read more...	•FedRAMP-Low-Revision-4: ac-2 read more...
INFO	medium	account	us-east-1	account_security_contact_information_is_registered	Ensure security contact information is registered.	390402539438		Manual check: Login to the AWS Console. Choose your account name on the top right of the window - > My Account - > Alternate Contacts -> Security Section.	AWS provides customers with th read more...	Go to the My Account section a read more...	•CIS-1.4: 1.2 •ENS-RD2022: o read more...
INFO	medium	account	us-east-1	account_security_questions_are_registered_in_the_aws_account	Ensure security questions are registered in the AWS account.	390402539438		Manual check: Login to the AWS Console as root. Choose your account name on the top right of the window - > My Account - > Configure Security Challenge Questions.	The AWS support portal allows read more...	Login as root account and from read more...	•CIS-1.4: 1.3 •ENS-RD2022: o read more...
FAIL	low	ssm	us-east-1	ssmincidents_enabled_with_plans	Ensure SSM Incidents is enabled with response plans.	390402539438		No SSM Incidents replication set exists.	Not having SSM Incidents enabl read more...	Enable SSM Incidents and creat read more...	•ENS-RD2022: op.exp.9.aws.img read more...
PASS	medium	fms	us-east-1	fms_policy_compliant	Ensure that all FMS policies inside an admin account are compliant	390402539438		FMS enabled with all compliant accounts.	If FMS policies are not compli read more...	Ensure FMS is enabled and all read more...	
FAIL	medium	vpc	us-east-1	vpc_different_regions	Ensure there are VPCs in more than one region	390402539438		VPCs found only in one region.		Ensure there are VPCs in more read more...	
INFO	medium	account	us-east-1	account_maintain_current_contact_details	Maintain current contact details.	390402539438		Manual check: Login to the AWS Console. Choose your account name on the top right of the window - > My Account - > Contact Information.	Ensure contact email and telep read more...	Using the Billing and Cost Man read more...	•CIS-1.4: 1.1 •ENS-RD2022: o read more...
FAIL	medium	account	us-east-1	account_maintain_different_contact_details_to_security_billing_and_operations	Maintain different contact details to security, billing and operations.	390402539438		SECURITY, BILLING and OPERATIONS contacts not found or they are not different between each other and between ROOT contact.	Ensure contact email and telep read more...	Using the Billing and Cost Man read more...	
FAIL	low	resourceexplorer2	us-east-1	resourceexplorer2_indexes_found	Resource Explorer Indexes Found	390402539438		No Resource Explorer Indexes found.	Not having Resource Explorer i read more...	Create indexes read more...	•ENS-RD2022: op.exp.1.aws.re.1