Cloud Conformity Infrastructure Report: CIS Amazon Web Services Foundations Benchmark v1.2.0

AWS Account: Master

Thu Apr 09 2020 17:58:25 GMT+0000 (Coordinated Universal Time)
CIS Benchmark (1 Account)

Summary

178 Filtered Checks 35% **62** Failed 65% **116** Succeeded#

Filters applied:
Standards & Frameworks: CIS Amazon Web Services Foundations Benchmark v1.2.0

#Compliance Score and percent success metrics are dependent on (1) active / selected filters, (2) data access you have provided on your account(s) or provided to you by your Organisation admin, and (3) controls which Cloud Conformity is able to check for on your cloud infrastructure - this would exclude for example workload across accounts, and organisational processes. Standard and framework control to rule mapping represents the expert opinion of Cloud Conformity and not necessarily that of the standard or framework authority. Rule severities and categories apply to Cloud Conformity's rules and not the controls they are mapped to. Your account(s) compliance with any Framework or Standard should be assessed in conjunction with your own internal review.

Identity and Access Management

Number	Recommendation	Profile	Total counts
1.1	Avoid the use of the "root" account	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Root Account Usage Updated	IAM	Security	High	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.2	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	Level 1	0

Rule	Service	Categories	Risk level	Counts
No rule to display				

Number	Recommendation	Profile	Total counts
1.3	Ensure credentials unused for 90 days or greater are disabled	Level 1	0

Rule	Service	Categories	Risk level	Counts
No rule to display				

Number	Recommendation	Profile	Total counts
1.4	Ensure access keys are rotated every 90 days or less	Level 1	0

Rule	Service	Categories	Risk level	Counts
No rule to display				

Number	Recommendation	Profile	Total counts
1.5	Ensure IAM password policy requires at least one uppercase letter	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Password Policy Uppercase	IAM	Security	Medium	SUCCESS: 1

Number	Recommendation	Profile	Total counts

1.6	Ensure IAM password policy require at least one lowercase letter	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Password Policy Lowercase	IAM	Security	Medium	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.7	Ensure IAM password policy require at least one symbol	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Password Policy Symbol	IAM	Security	Medium	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.8	Ensure IAM password policy require at least one number	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Password Policy Number	IAM	Security	Medium	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.9	Ensure IAM password policy requires minimum length of 14 or greater	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Password Policy Minimum Length	IAM	Security	Medium	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.10	Ensure IAM password policy prevents password reuse	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Password Policy Reuse Prevention	IAM	Security	Medium	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.11	Ensure IAM password policy expires passwords within 90 days or less	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Password Policy Expiration	IAM	Security	Medium	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.12	Ensure no root account access key exists	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Root Account Access Keys Present	IAM	Security	High	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.13	Ensure MFA is enabled for the "root" account	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Root MFA Enabled	IAM	Security	High	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.14	Ensure hardware MFA is enabled for the "root" account	Level 2	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Hardware MFA for AWS Root Account	IAM	Security	High	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.15	Ensure security questions are registered in the AWS account	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Account Security Challenge Questions (Not Scored)	IAM	Security	High	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.16	Ensure IAM policies are attached only to groups or roles	Level 1	0

Rule	Service	Categories	Risk level	Counts
No rule to display				

Number	Recommendation	Profile	Total counts
1.17	Maintain current contact details	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts

Current Contact Details (Not Scored)	Budgets	Security	Medium	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.18	Ensure security contact information is registered	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Account Alternate Contacts (Not Scored)	IAM	Security	High	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.19	Ensure IAM instance roles are used for AWS resource access from instances	Level 2	0

Rule	Service	Categories	Risk level	Counts
No rule to display				

Number	Recommendation	Profile	Total counts
1.20	Ensure a support role has been created to manage incidents with AWS Support	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Support Role	IAM	Security	High	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.21	Do not setup access keys during initial user setup for all IAM users that have a console password	Level 1	SUCCESS: 1

Rule	Service	Categories	Risk level	Counts
Access Keys During Initial IAM User Setup (Not Scored)	IAM	Security	Medium	SUCCESS: 1

Number	Recommendation	Profile	Total counts
1.22	Ensure IAM policies that allow full "*:*" administrative privileges are not created	Level 1	SUCCESS: 4

Rule	Service	Categories	Risk level	Counts
IAM Policies With Full Administrative Privileges	IAM	Security	High	SUCCESS: 4

Logging

Number	Recommendation	Profile	Total counts
2.1	Ensure CloudTrail is enabled in all regions	Level 1	SUCCESS: 16

Rule	Service	Categories	Risk level	Counts
CloudTrail Enabled	CloudTrail	Security	High	SUCCESS: 16

Number	Recommendation	Profile	Total counts
2.2	Ensure CloudTrail log file validation is enabled	Level 2	SUCCESS: 16

Rule	Service	Categories	Risk level	Counts
CloudTrail Log File Integrity Validation	CloudTrail	Security	Medium	SUCCESS: 16

Number	Recommendation	Profile	Total counts
2.3	Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible	Level 1	0

Rule	Service	Categories	Risk level	Counts
No rule to display				

Number	Recommendation	Profile	Total counts
2.4	Ensure CloudTrail trails are integrated with CloudWatch Logs	Level 1	SUCCESS: 16

Rule	Service	Categories	Risk level	Counts
CloudTrail Integrated With CloudWatch	CloudTrail	Security	Medium	SUCCESS: 16

Number	Recommendation	Profile	Total counts
2.5	Ensure AWS Config is enabled in all regions	Level 1	SUCCESS: 16

Rule	Service	Categories	Risk level	Counts
AWS Config Enabled	Config	Security	High	SUCCESS: 16

Number	Recommendation	Profile	Total counts

2.6	Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket	Level 1	0

Rule	Service	Categories	Risk level	Counts
No rule to display				

Number	Recommendation	Profile	Total counts
2.7	Ensure CloudTrail logs are encrypted at rest using KMS CMKs	Level 2	FAILURE: 16

Rule	Service	Categories	Risk level	Counts	
CloudTrail Logs Encrypted	CloudTrail	Security	Medium	FAILURE: 16	Resolve...

Number	Recommendation	Profile	Total counts
2.8	Ensure rotation for customer created CMKs is enabled	Level 2	0

Rule	Service	Categories	Risk level	Counts
No rule to display				

Number	Recommendation	Profile	Total counts
2.9	Ensure VPC flow logging is enabled in all VPCs	Level 2	FAILURE: 16

Rule	Service	Categories	Risk level	Counts	
VPC Flow Logs Enabled	VPC	Security	Low	FAILURE: 16	Resolve...

Monitoring

Number	Recommendation	Profile	Total counts
3.1	Ensure a log metric filter and alarm exist for unauthorized API calls	Level 1	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
Authorization Failures Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.2	Ensure a log metric filter and alarm exist for Management Console sign-in without MFA	Level 1	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
AWS Console Sign In Without MFA	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.3	Ensure a log metric filter and alarm exist for usage of "root" account	Level 1	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
Root Account Usage Alarm	CloudWatchLogs	Security	High	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.4	Ensure a log metric filter and alarm exist for IAM policy changes	Level 1	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
IAM Policy Changes Alarm	CloudWatchLogs	Security	High	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.5	Ensure a log metric filter and alarm exist for CloudTrail configuration changes	Level 1	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
CloudTrail Changes Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.6	Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	Level 2	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
Console Sign-in Failures Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.7	Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs	Level 2	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
CMK Disabled or Scheduled for Deletion Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.8	Ensure a log metric filter and alarm exist for S3 bucket policy changes	Level 1	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
S3 Bucket Changes Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.9	Ensure a log metric filter and alarm exist for AWS Config configuration changes	Level 2	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
AWS Config Changes Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.10	Ensure a log metric filter and alarm exist for security group changes	Level 2	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
Security Group Changes Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.11	Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	Level 2	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
Network ACL Changes Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.12	Ensure a log metric filter and alarm exist for changes to network gateways	Level 1	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
Internet Gateway Changes Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.13	Ensure a log metric filter and alarm exist for route table changes	Level 1	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
Route Table Changes Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Number	Recommendation	Profile	Total counts
3.14	Ensure a log metric filter and alarm exist for VPC changes	Level 1	FAILURE: 1

Rule	Service	Categories	Risk level	Counts	
VPC Changes Alarm	CloudWatchLogs	Security	Medium	FAILURE: 1	Resolve...

Networking

Number	Recommendation	Profile	Total counts
4.1	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	Level 1	SUCCESS: 16

Rule	Service	Categories	Risk level	Counts
Unrestricted SSH Access	EC2	Security	Medium	SUCCESS: 16

Number	Recommendation	Profile	Total counts
4.2	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	Level 1	SUCCESS: 16

Rule	Service	Categories	Risk level	Counts
Unrestricted RDP Access	EC2	Security	Medium	SUCCESS: 16

Number	Recommendation	Profile	Total counts
4.3	Ensure the default security group of every VPC restricts all traffic	Level 2	FAILURE: 16

Rule	Service	Categories	Risk level	Counts	
Default Security Group Unrestricted	EC2	Security	Low	FAILURE: 16	Resolve...

Number	Recommendation	Profile	Total counts
4.4	Ensure routing tables for VPC peering are "least access"	Level 2	0

Rule	Service	Categories	Risk level	Counts

No rule to display